**BURSOR & FISHER, P.A.**
Philip L. Fraietta (State Bar No. 354768)
Max S. Roberts (*Pro Hac Vice Forthcoming*)
Victoria X. Zhou (*Pro Hac Vice Forthcoming*)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com
mroberts@bursor.com
vzhou@bursor.com

**BURSOR & FISHER, P.A.**
Joshua R. Wilner (State Bar No. 353949)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: jwilner@bursor.com

*Attorneys for Plaintiffs*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

ZHICHENG ZHEN, MARCUS JOHNSON, JANE DOE, MARC RUSSO, DILARA USKUP, and KELDA MCKINNEY, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

EXPERIAN DATA CORPORATION, EXPERIAN INFORMATION SOLUTIONS, INC., EXPERIAN PLC, and TAPAD, INC.,

Defendants.

Case No.

**CLASS ACTION COMPLAINT**

**<u>JURY TRIAL DEMANDED</u>**

# TABLE OF CONTENTS

PAGE

Plaintiffs ZhiCheng Zhen, Marcus Johnson, Jane Doe, Kelda McKinney, Dilara Uskup, and Marc Russo ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Experian PLC, Experian Data Corporation, Experian Information Solutions, Inc. (together, "Experian"), and Tapad, Inc. ("Tapad") (all together, "Defendants"). Plaintiffs bring this action based upon personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

## NATURE OF THE ACTION

1. This class action lawsuit sets forth how the business practices of Experian and Tapad amount to a deliberate surveillance of millions of Americans via their activity on the Internet and mobile applications. Experian, through Tapad, tracks in real time and records indefinitely the personal information and specific web activity of hundreds of millions of Americans.

2. This unlawfully collected information is worth billions of dollars to Defendants because it makes up the content of Experian's ID Graph, Consumer View, and Consumer Sync products, and creates individual sales of advertisements in the real-time-bidding ecosystem present on thousands of major websites.

3. Plaintiffs bring this action to enforce their constitutional rights to privacy and to seek damages under California law for the harm caused by the collection and sale of their confidential data and personal information.

## THE PARTIES

### I. PLAINTIFFS

4. ***Plaintiff ZhiCheng Zhen.*** Plaintiff ZhiCheng Zhen is a natural person and citizen of California, residing in Oakland, California. Plaintiff Zhen was in California when he accessed the GEICO website and had his activity on that website and subsequent activity on other websites tracked by Defendants.

5. ***Plaintiff Marcus Johnson.*** Plaintiff Marcus Johnson is a natural person and citizen of California, residing in Oakland, California. Plaintiff Johnson was in California when he accessed the GEICO website and had his activity on that website and subsequent activity on other websites tracked by Defendants.

6. ***Plaintiff Jane Doe.*** Plaintiff Jane Doe is a natural person and citizen of California, residing in Milford, California. Plaintiff Doe was in California when she made a purchase on the Mindbloom website and had her activity on that website and subsequent activity on other websites tracked by Defendants.[1]

7. ***Plaintiff Kelda McKinney.*** Plaintiff Kelda McKinney is a natural person and citizen of California, residing in Oakland, California. Plaintiff McKinney was in California when she accessed the Loan Depot website and had her activity on that website and subsequent activity on other websites tracked by Defendants.

8. ***Plaintiff Dilara Uskup.*** Plaintiff Dilara Uskup is a natural person and citizen of California, residing in Los Angeles, California. Plaintiff Uskup was in California when she accessed the Zillow website and had her activity on that website and subsequent activity on other websites tracked by Defendants.

9. ***Plaintiff Marc Russo.*** Plaintiff Marc Russo is a natural person and citizen of California, residing in San Diego, California. Plaintiff Russo was in California when he applied for a loan on the Rocket Mortgage website and had his activity on that website, confidential communications with the website, and activity on other websites tracked by Defendants.

## II. DEFENDANTS

10. ***Defendant Experian PLC.*** Defendant Experian PLC is a company formed under the laws of Ireland with its principal place of business at 2 Cumberland Place, Fenian Street, Dublin 2, D02 HY05, Ireland. Experian PLC is the global parent company of the other Defendants and directly controls their operations in the United States.

11. ***Defendant Experian Data Corporation.*** Defendant Experian Data Corporation is a Delaware corporation with its principal place of business at 475 Anton Blvd., Costa Mesa, California 92626. Experian Data Corporation directly controls Tapad's activities, uses Tapad's technology to enhance its products, and integrates data collected by Tapad into datasets and products it sells to third parties.

[1] Because Plaintiff Doe accessed the Mindbloom website, which provides ketamine therapy, and ketamine is a Schedule III drug pursuant to the Controlled Substances Act (21 U.S.C. §§ 801, *et seq.*), Plaintiff Doe's name has been anonymized to protect her privacy.

12. ***Defendant Experian Information Solutions, Inc.*** Defendant Experian Information Solutions, Inc. is an Ohio corporation with its principal place of business at 475 Anton Blvd., Costa Mesa, California 92626. Experian Information Solutions, Inc. directly controls Tapad's activities, uses Tapad's technology to enhance its products, and integrates data collected by Tapad into datasets and products it sells to third parties.

13. ***Defendant Tapad, Inc.*** Defendant Tapad, Inc. is a Delaware corporation with its principal place of business at 261 Madison Avenue, 4th Floor, New York, New York 10016. Tapad is wholly owned by Experian and Experian directs the actions of Tapad, uses Tapad's technology to accomplish the widespread surveillance alleged herein, and has access to all information collected by Tapad.

## JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from at least one Defendant.

15. This Court has personal jurisdiction over Defendants because Defendants collected the private information of thousands or millions of people in California, sold that information to advertisers in California—who targeted advertisements to Californians based in part on their location in California—and profited from the sale of Californians' personal information. Further, Defendants Experian Data Corporation and Experian Information Solutions have their principal place of business in California.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to the claim occurred in this District.

## FACTUAL ALLEGATIONS

### I. DATA BROKERS AND REAL-TIME BIDDING: THE INFORMATION ECONOMY

17. To put the invasiveness of Defendants' privacy violations into perspective, it is important to understand two concepts: data brokers and real-time bidding.

### A. Data Brokers

18. While "[t]here is no single, agreed-upon definition of data brokers in United States law,"[2] California law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct [*i.e.*, consumer-facing] relationship," subject to certain exceptions. Cal. Civ. Code § 1798.99.80(c).

19. Any entity that qualifies as a "data broker" under California law must specifically register as such (Cal. Civ. Code § 1798.99.82(a)), which both Experian[3] and Tapad[4] do.

20. "Data brokers typically offer pre-packaged databases of information to potential buyers," either through the "outright s[ale of] data on individuals" or by "licens[ing] and otherwise shar[ing] the data with third parties."[5] Such databases are extensive, and can "not only include information publicly available [such as] from Facebook but also the user's exact residential address, date and year of birth, and political affiliation," in addition to "inferences [that] can be made from the combined data." And whereas individual data sources "may provide only a few elements about a person's activities, data brokers combine these elements to form a detailed, composite view of the consumer's life."[6]

21. For instance, as a report by NATO found, data brokers like Defendants collect two sets of information: "observed and inferred (or modelled)." The former "is data that has been collected and is actual," such as websites visited." Inferred data "is gleaned from observed data by modelling or profiling," meaning what consumers may be *expected* to do. On top of this, "[b]rokers

[2] JUSTIN SHERMAN, DUKE SANFORD CYBER POLICY PROGRAM, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS: THREATS TO AMERICAN CIVIL RIGHTS, NATIONAL SECURITY, AND DEMOCRACY, at 2 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

[3] DATA BROKER REGISTRATION FOR EXPERIAN INFORMATION SOLUTIONS, INC., https://oag.ca.gov/data-broker/registration/186691.

[4] DATA BROKER REGISTRATION FOR TAPAD, INC., https://oag.ca.gov/data-broker/registration/187511.

[5] SHERMAN, *supra*, at 2.

[6] Tehila Minkus et al., *The City Privacy Attack: Combining Social Media and Public Records for Detailed Profiles of Adults and Children*, COSN '15: PROCEEDINGS OF THE 2015 ACM ON CONFERENCE ON ONLINE SOCIAL NETWORKS 71, 71 (2015), https://dl.acm.org/doi/pdf/10.1145/2817946.2817957.

typically collect not only what they immediately need or can use, but hoover up as much information as possible to compile comprehensive data sets that might have some future use."[7]

22. Likewise, a report by the Duke Sanford Cyber Policy Program "examine[d] 10 major data brokers [including Experian] and the highly sensitive data they hold on U.S. individuals."[8] The report found that "data brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees."[9]

23. Indeed, as the Duke Sanford report noted, Experian "processes over 2 billion records monthly and has over 8 billion name and address combinations, with the ability to convert sensitive [] personally identifiable information data into actionable insights."[10]

24. According to the Duke Sanford report, Experian "advertises data on 95% of the U.S. population … spanning thousands of attributes." Experian does so by "ingest[ing] first-party data such as names, physical addresses, email addresses, mobile ad identifiers (MAIDs), IP addresses, and other information to link economic transactions to an Experian household ID. It advertises mobile location data on users and the ability to link information to 500 million email addresses and 275 million addressable cookies."[11]

25. This data collection has grave implications for Americans' right to privacy. For instance, "U.S. federal agencies from the Federal Bureau of Investigation [] to U.S. Immigration and Customs Enforcement [] purchase data from data brokers—without warrants, public disclosures, or robust oversight—to carry out everything from criminal investigations to deportations."[12]

[7] HENRIK TWETMAN & GUNDARS BERGMANIS-KORATS, NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, DATA BROKERS AND SECURITY at 11 (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[8] SHERMAN, *supra*, at 1.

[9] *Id.*

[10] *Id.* at 6 (cleaned up).

[11] *Id.* (cleaned up).

[12] *Id.* at 9.

26. As another example:

> Data brokers also hold highly sensitive data on U.S. individuals such as race, ethnicity, gender, sexual orientation, immigration status, income level, and political preferences and beliefs (like support for the NAACP or National LGBTQ Task Force) that can be used to directly undermine individuals' civil rights. Even if data brokers do not explicitly advertise these types of data (though in many cases they do), everything from media reporting to testimony by a Federal Trade Commission commissioner has identified the risk that data brokers use their data sets to make "predictions" or "inferences" about this kind of sensitive information (race, gender, sexual orientation, etc.) on individuals.
>
> This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements. 59 Many industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services.
>
> …
>
> Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups.[13]

27. Similarly, as the report from NATO noted, corporate data brokers cause numerous privacy harms, including but not limited to depriving consumers of the right to control who does and does not acquire their personal information, unwanted advertisements that can even go as far as manipulating viewpoints, and spam and phishing attacks.[14]

//

//

//

//

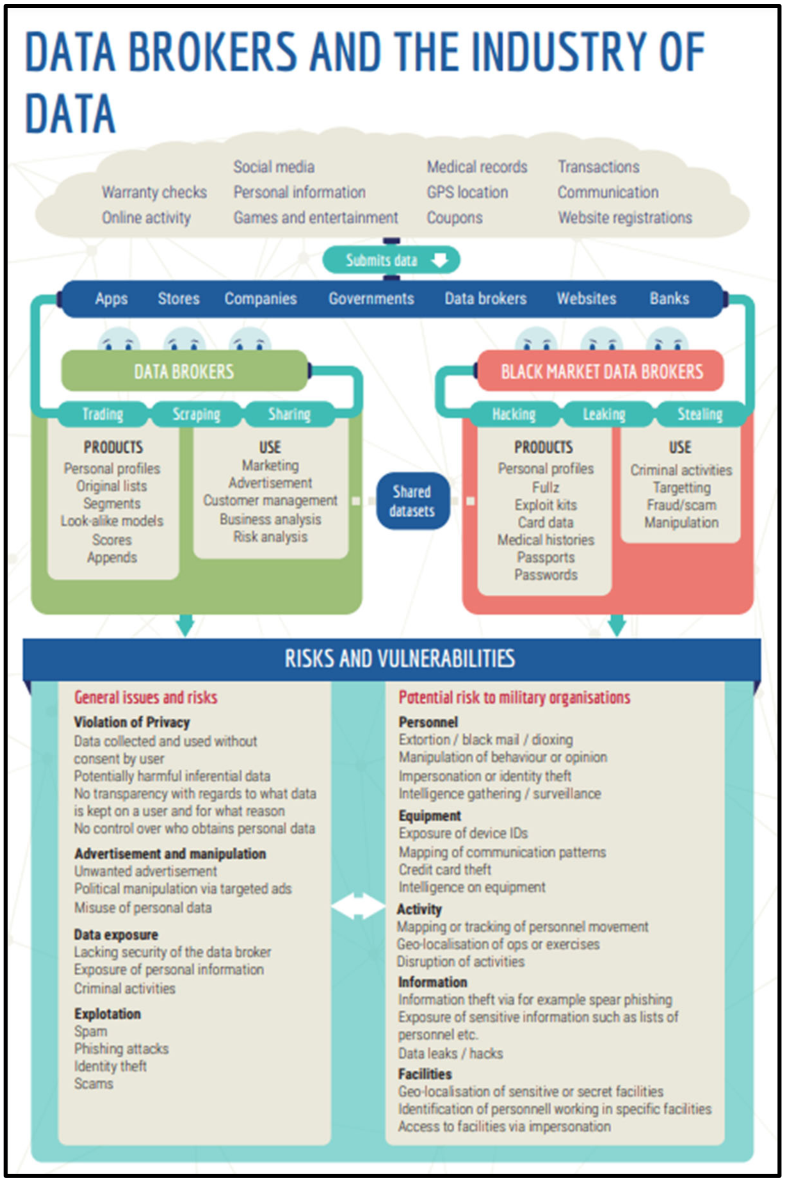
//

//

//

[13] *Id.*

[14] TWETMAN & BERGMANIS-KORATS, *supra*, at 8.



General issues and risks

**Violation of Privacy**
Data collected and used without consent by user
Potentially harmful inferential data
No transparency with regards to what data is kept on a user and for what reason
No control over who obtains personal data

**Advertisement and manipulation**
Unwanted advertisement
Political manipulation via targeted ads
Misuse of personal data

**Data exposure**
Lacking security of the data broker
Exposure of personal information
Criminal activities

**Explotation**
Spam
Phishing attacks
Identity theft
Scams

Potential risk to military organisations

**Personnel**
Extortion / black mail / dioxing
Manipulation of behaviour or opinion
Impersonation or identity theft
Intelligence gathering / surveillance

**Equipment**
Exposure of device IDs
Mapping of communication patterns
Credit card theft
Intelligence on equipment

**Activity**
Mapping or tracking of personnel movement
Geo-localisation of ops or exercises
Disruption of activities

**Information**
Information theft via for example spear phishing
Exposure of sensitive information such as lists of personnel etc.
Data leaks / hacks

**Facilities**
Geo-localisation of sensitive or secret facilities
Identification of personnell working in specific facilities
Access to facilities via impersonation

28. Data brokers like Defendants are able to compile such wide swaths of information in part by collecting users' IP addresses and other device information, which is used by data brokers like Defendants to track users across the Internet.[15] Indeed, as McAfee (a data security company) notes, "data brokers can … even place trackers or cookies on your browsers … [that] track your IP address and browsing history, which third parties can exploit."[16]

[15] *Id.* at 11.

[16] Jasdev Dhaliwal, *How Data Brokers Sell Your Identity*, MCAFEE (June 4, 2024), https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/.

29. These data brokers will then:

> take that data and pair it with other data they've collected about you, pool it together with other data they've got on you, and then share all of it with businesses who want to market to you. They can eventually build large datasets about you with things like: "browsed gym shorts, vegan, living in Los Angeles, income between $65k-90k, traveler, and single." Then, they sort you into groups of other people like you, so they can sell those lists of like-people and generate their income.[17]

30. In short, data brokers like Defendants track consumers across the Internet, compiling various bits of information about users, building comprehensive user profiles that include an assortment of information, interests, and inferences, and offering up that information for sale to the highest bidder. The "highest bidder" is a literal term, as explained below.

### B. Real-Time Bidding

31. So, once data brokers like Defendants collect information from consumers and create comprehensive user profiles, how do Defendants "sell" or otherwise monetize that information? This is where real-time bidding comes in.

32. "Real Time Bidding (RTB) is an online advertising auction that uses sensitive personal information to facilitate the process to determine which digital ad will be displayed to a user on a given website or application."[18]

33. "There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs)." An SSP "work[s] with website or app publishers to help them participate in the RTB process." "DSPs primarily work with advertisers to help them evaluate the value of user impressions and optimize the bid prices they put forth."[19] And an Advertising Exchange "allows advertisers and publishers to use the same technological platform, services, and methods, and "speak the same language" in order to exchange data, set prices, and ultimately serve an ad."[20]

[17] Paul Jarvis, *The Problem with Data Brokers: Targeted Ads and Your Privacy*, FATHOM ANALYTICS (May 10, 2022), https://usefathom.com/blog/data-brokers.

[18] Sara Geoghegan, *What is Real Time Bidding?*, ELECTRONIC PRIVACY INFORMATION CENTER (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/.

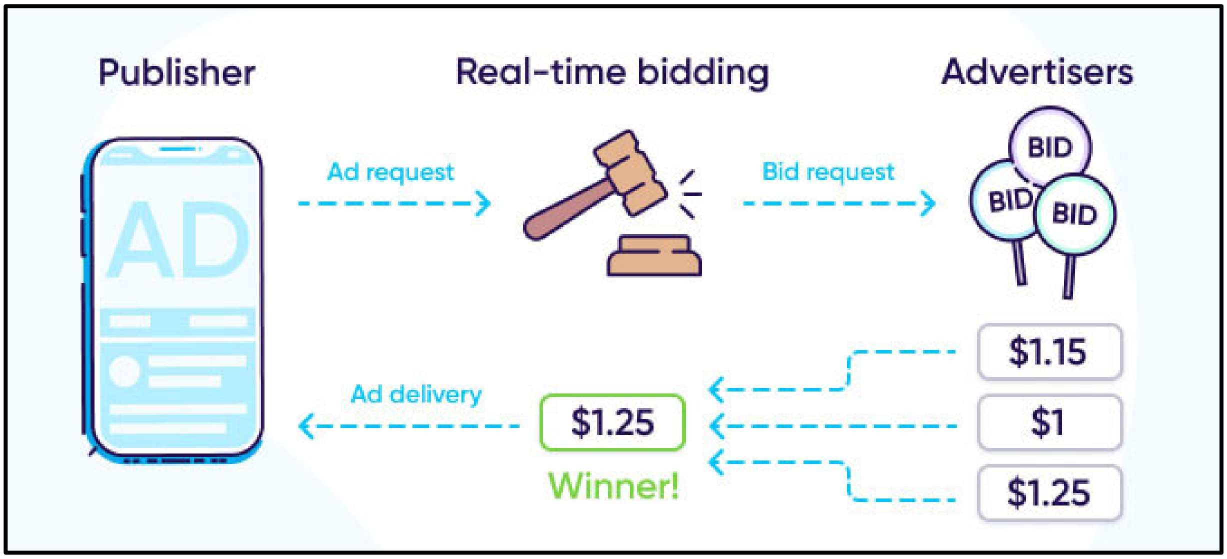
[19] Geoghegan, *supra*.

[20] *Introducing To Ad Serving*, MICROSOFT IGNITE (Mar. 3, 2024), https://learn.microsoft.com/en-us/xandr/industry-reference/introduction-to-ad-serving.

34. In other words, SSPs provide user information to advertisers that might be interested in those users, DSPs help advertisers select which users to advertise and target, and an Advertising Exchange is the platform on which all of this happens.

35. The RTB process works as follows:

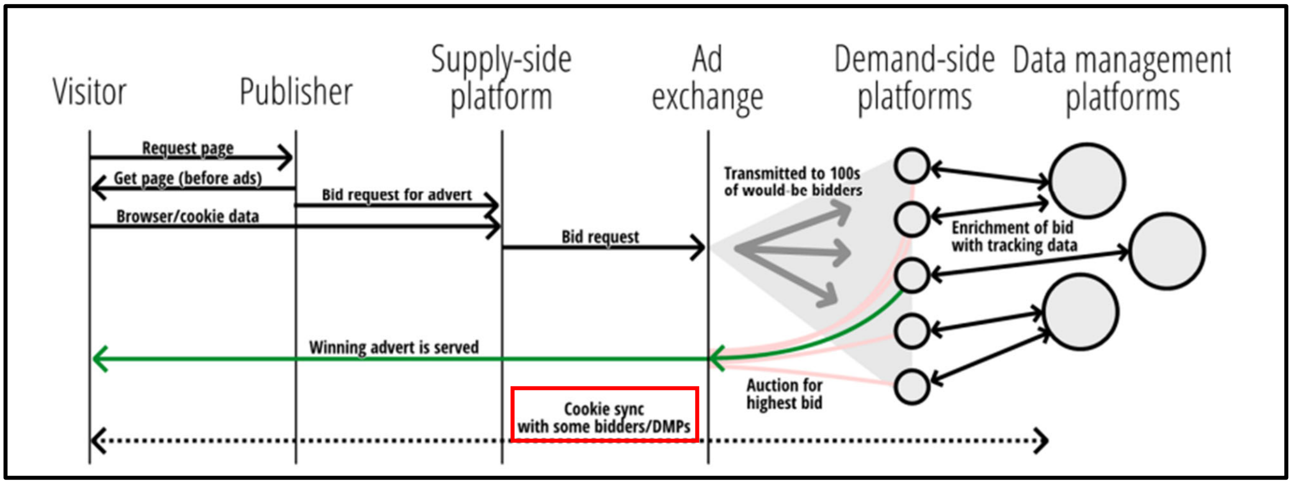
> After a user loads a website or app, an SSP will send user data to Advertising Exchanges … The user data, often referred to as "bidstream data," contains information like device identifiers, IP address, zip/postal code, GPS location, browsing history, location data, and more. After receiving the bidstream data, an Advertising Exchange will broadcast the data to several DSPs. The DSPs will then examine the broadcasted data to determine whether to make a bid on behalf of their client.
>
> Ultimately, if the DSP wins the bid, its client's advertisement will appear to the user. Since most RTB auctions are held on the server/exchange side, instead of the client/browser side, the user only actually sees the winner of the auction and would not be aware of the DSPs who bid and lost. But even the losing DSPs still benefit because they also receive and collect the user data broadcasted during the RTB auction process. This information can be added to existing dossiers DSPs have on a user.[21]



36. Facilitating this real-time bidding process means SSPs and DSPs must have as much information as possible about consumers to procure the greatest interest from advertisers and obtain the highest bids for website and app operators' users. But these SSPs and DSPs receive assistance by connecting with Data Management Platforms ("DMPs") or data brokers like Defendants:

[21] Geoghegan, *supra*; *see also* REAL-TIME BIDDING, APPSFLYER, https://www.appsflyer.com/glossary/real-time-bidding/.

> the economic incentives of an auction mean that DSP with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The DSP enlists a final actor, the data management platform (DMP) [here, Defendants]. DSPs send bid requests to DMPs, who enrich them by attempting to identify the user in the request and use a variety of data sources, such as those uploaded by the advertiser, collected from other sources, or bought from data brokers The DSP also wins the right to cookie sync its own cookies with those from the [Advertising Exchange], thus enabling easier linkage of the data to the user's profile in the future.[22]



37. In other words, before bidding to show a user an advertisement, a DSP will attempt to determine what other information about a user may be available. A DSP does this by connecting with entities like Defendants, who match a consumer's information from a particular website or mobile application (*e.g.*, their IP address) with any profiles on those users Defendants may have compiled. If there is a match, then advertisers will pay more money to show users an advertisement because the advertisers have more information to base their targeting on. This naturally enriches website and app operators, as their users are now more valuable. And, a DSP is able to continue linking users on a website or mobile application through the Advertising Exchange, which enhances the DSP's ability to better identify users in the future and helps the DSP profit further as well.

38. As the Federal Trade Commission ("FTC") has noted, "[t]he use of real-time bidding presents potential concerns," including but not limited to:

[22] Michael Veale & Federik Zuiderveen Borgesius, *Adtech and Real-Time Bidding under European Data Protection Law*, 23 GERMAN L. J. 226, 232-33 (2022) https://tinyurl.com/yjddt5ey. The red box shows where a data broker like Defendants will be called in the RTB process.

(a) "incentiviz[ing] invasive data-sharing" by "push[ing] publishers [*i.e.*, website and app operators] to share as much end-user data as possible to get higher valuation for their ad inventory—particularly their location data and cookie cache, which can be used to ascertain a person's browsing history and behavior."

(b) "send[ing] sensitive data across geographic borders."

(c) sending consumer data "to potentially dozens of bidders simultaneously, despite only one of those parties—the winning bidder actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring those other parties do not retain that data for use in unintended ways."[23]

39. The last point bears additional emphasis, as it means the data Defendants provide to DSPs to serve targeted advertisements is even provided to those entities who do not actually serve an advertisement on a consumer. This greatly diminishes the ability of users to control their personal information.

40. Likewise, the Electronic Privacy Information Center ("EPIC") has warned that "[c]onsumers' privacy is violated when entities disclose their information without authorization or in ways that thwart their expectations."[24]

41. All of this is in line with protecting the right to determine who does and does not get to know one's information, a harm long recognized at common law and one statutes like the CIPA were enacted to protect against. *Ribas v. Clark*, 38 Cal. 3d 355, 361 (1985) (noting the CIPA was drafted with a two-party consent requirement to protect "the right to control the nature and extent of the firsthand dissemination of [one's] statements"); *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763-64 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

* * *

[23] FEDERAL TRADE COMMISSION, UNPACKING REAL TIME BIDDING THROUGH FTC'S CASE ON MOBILEWALLA (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla.

[24] Geoghegan, *supra*.

42. To summarize the proceeding allegations, website and mobile application operators monetize their platforms through the user of real-time bidding. Through this process, consumer information is provided to advertisers who are interested in showing advertisements to particular consumers. Advertisers then "bid" to show consumers an advertisement, with the winning bidder ultimately having their advertisement displayed to consumers. However, all interested advertisers receive consumers' information regardless.

43. The value of those users is enriched by partnering with data brokers or data management platforms like Defendants, which enables those entities involved in RTB to link the information said entities collect from consumers on a particular website or app with Defendants' vast repository of information and user profiles that Defendants maintain on billions of consumers. This enriches the value a website or app's user base because advertisers have a wider swath of information to use to target relevant consumers, meaning advertisers will pay more money to show users an advertisement on that website or application.

44. Of course, Defendants also benefit from this arrangement because websites and apps will want to employ Defendants' services to bring in more advertising revenue, meaning Defendants can continue to expand and grow the information they have about any consumers and add to consumers' profiles, which further perpetuates the value of Defendants' services.

45. As it stands though, Defendants, individually and in combination under the Experian umbrella, are already one of the largest players in this industry. Defendants achieved this status through the use of a variety of technologies and services, as described below.

## II. AN OVERVIEW OF DEFENDANTS' SERVICES

### A. Tapad

46. Defendant Tapad—who, as noted above, is a registered data broker in California—was founded in 2010 by Are Traasdahl with the explicit intention of developing technology that would "track and target the same consumer across multiple devices."[25]

[25] https://www.forbes.com/sites/jjcolao/2013/05/23/ads-that-follow-you-home-has-Tapad-cracked-the-code-of-cross-device-advertising/ (last visited Dec. 23, 2024).

47. Tapad achieves this by “crunching 150 billion data points—from cookies, cellphone IDs (which link individual phones to app downloads and Web browsing), Wi-Fi connections, website registrations, browsing history and other inputs.”[26]

48. Tapad aggregated these inputs into what it called a “Device Graph,” which allowed advertisers to connect individuals to all the devices those individuals use for the purpose of delivering targeted advertisements.[27]

49. Over the next decade, Tapad’s proprietary tracking technology was honed with the assistance of several rounds of investments and acquisitions. By 2016, Tapad worked with 160 brands and 50 data licensing partners in the United States to track and serve advertising to millions of Americans.[28]

50. In 2020, Tapad was acquired by Experian for $280 million.[29] As alleged above, Experian is also a registered data broker in California that “has access to behavioral and demographic data on more than 300 million Americans across 125 million households and 2 billion devices.”[30] This acquisition “combine[d] Experian’s offline consumer data set (purchase behaviors, interests, lifestyle info) with [Tapad’s] online consumer data (media consumption habits and device usage)” to “bolster[] Experian’s ad tech and engineering know-how and gave the company a stronger foothold in the advertising ecosystem.”[31]

51. Indeed, both Experian’s “Consumer Sync”—which is for “hygiene, identity resolution and data collaboration”—and Consumer View—which is for “insights and activation”—#

[26] *Id.*

[27] https://techcrunch.com/2016/02/01/telenor-jumps-into-ad-tech-acquires-Tapad-for-360m/ (last visited Dec. 23, 2024).

[28] *Id.*

[29] Allison Schiff, *Telenor Sells Tapad to Experian for $280 Million*, ADEXCHANGER (Nov. 19, 2020), https://www.adexchanger.com/privacy/telenor-sells-Tapad-to-experian-for-280-million/.

[30] Anthony Vargas, *How Experian is Using Tapad to Build New ID Resolution and Analytics Products*, ADEXCHANGER (Feb. 21, 2023), https://www.adexchanger.com/data-exchanges/how-experian-is-using-Tapad-to-build-new-id-resolution-and-analytics-products/ (last visited Dec. 23, 2024).

[31] *Id.*

sit within Experian's marketing services division and were built using Tapad's technology as the foundation."[32]

### 1. *Tapad's Online Tracking Technology*

52. Tapad oversees a massive web of online tracking technologies that provide ongoing information to Tapad and Experian.

53. It is estimated that Tapad collected information on 1% of all web traffic—which constitutes *hundreds of billions of website interactions*—in July 2024 alone.[33]

54. The collection of this highly detailed information relies on a series of "pixels" loaded onto websites.

55. A pixel is a piece of code that website operators can integrate into their websites to "tracks the people and type of actions they take."[34]

56. Tapad collects information on Internet users' activity on a wide variety of websites through the use of several pixels it owns and develops.

57. The advertisers that Tapad contracts with have their own pixels, which are integrated into the design of websites. To facilitate the identity resolution process, described below, these pixels "call" (load) the pixels owned by Tapad onto the website.

58. The pixels Plaintiffs are aware of at this time that engage in this practice include but are not limited to the Snap Pixel, Criteo Pixel, Rubicon Pixel, Magellan Pixel, TripleLift Pixel, Pubmatic Pixel, (all owned by companies of the same name), the Adroll Pixel (owned by NextRoll), the Crowd Control Pixel (owned by Lotame), and the Adsrvr Pixel (owned by The Trade Desk) (all together, the "Partner Pixels"). However, there are likely many more Partner Pixels.

//

//

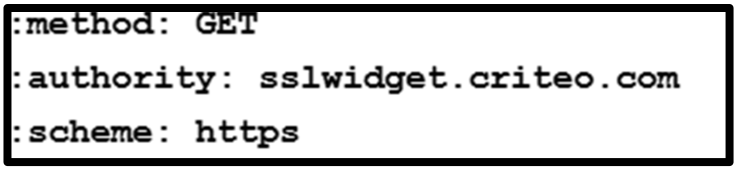
//

//

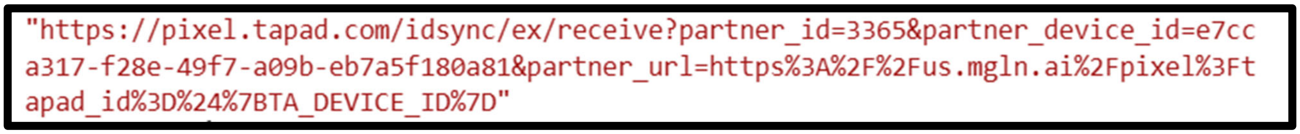
[32] *Id.*

[33] https://www.ghostery.com/whotracksme/trackers/Tapad (last visited Dec. 23, 2024).

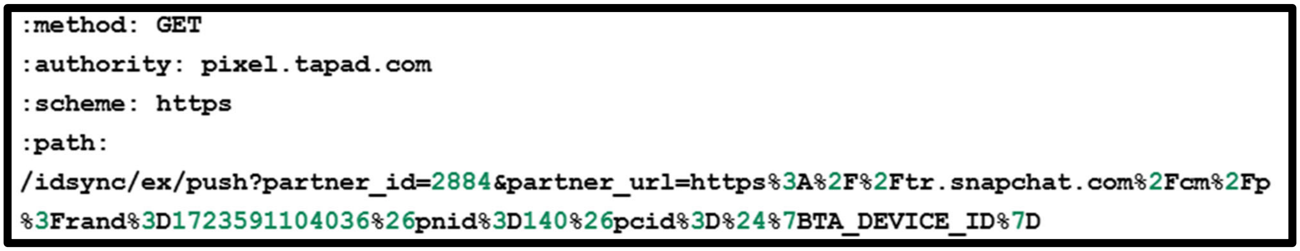
[34] https://www.facebook.com/business/goals/retargeting (last visited Dec. 23, 2024).



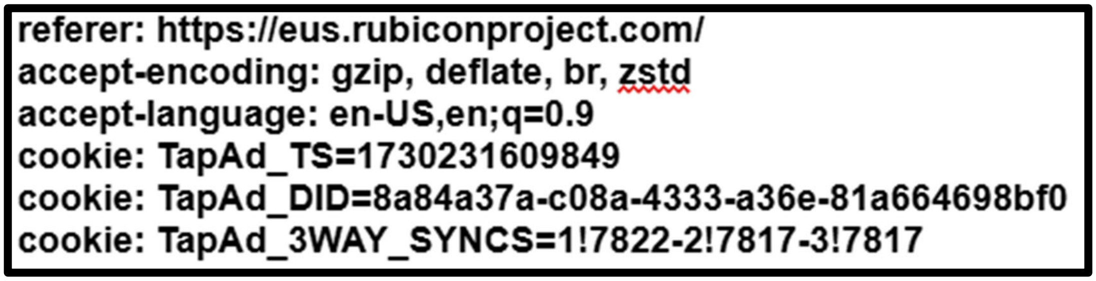
```
:method: GET
:authority: sslwidget.criteo.com
:scheme: https
```



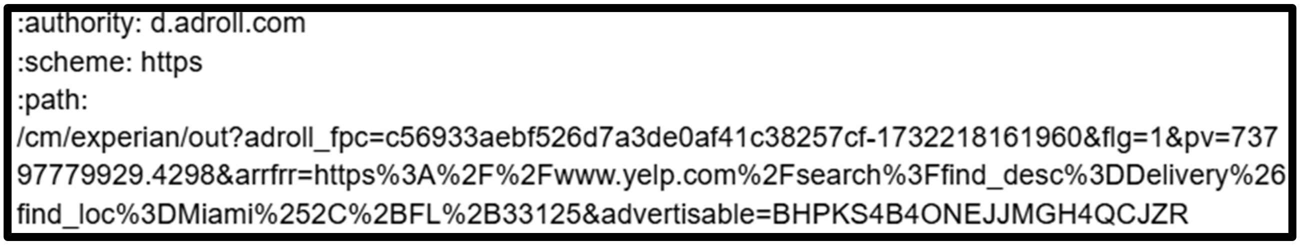
```
"https://pixel.tapad.com/idsync/ex/receive?partner_id=3365&partner_device_id=e7cc
a317-f28e-49f7-a09b-eb7a5f180a81&partner_url=https%3A%2F%2Fus.mgln.ai%2Fpixel%3Ft
apad_id%3D%24%7BTA_DEVICE_ID%7D"
```



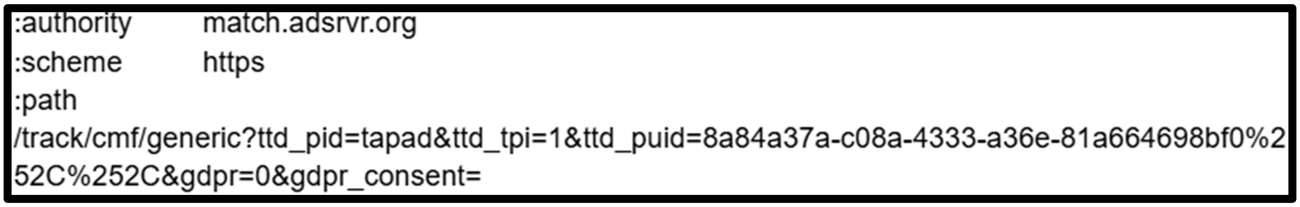
```
:method: GET
:authority: pixel.tapad.com
:scheme: https
:path:
/idsync/ex/push?partner_id=2884&partner_url=https%3A%2F%2Ftr.snapchat.com%2Fcm%2Fp
%3Frand%3D1723591104036%26pnid%3D140%26pcid%3D%24%7BTA_DEVICE_ID%7D
```



```
referer: https://eus.rubiconproject.com/
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cookie: TapAd_TS=1730231609849
cookie: TapAd_DID=8a84a37a-c08a-4333-a36e-81a664698bf0
cookie: TapAd_3WAY_SYNCS=1!7822-2!7817-3!7817
```



```
:authority: d.adroll.com
:scheme: https
:path:
/cm/experian/out?adroll_fpc=c56933aebf526d7a3de0af41c38257cf-1732218161960&flg=1&pv=737
97779929.4298&arrfrr=https%3A%2F%2Fwww.yelp.com%2Fsearch%3Ffind_desc%3DDelivery%26
find_loc%3DMiami%252C%2BFL%2B33125&advertisable=BHPKS4B4ONEJJMGH4QCJZR
```

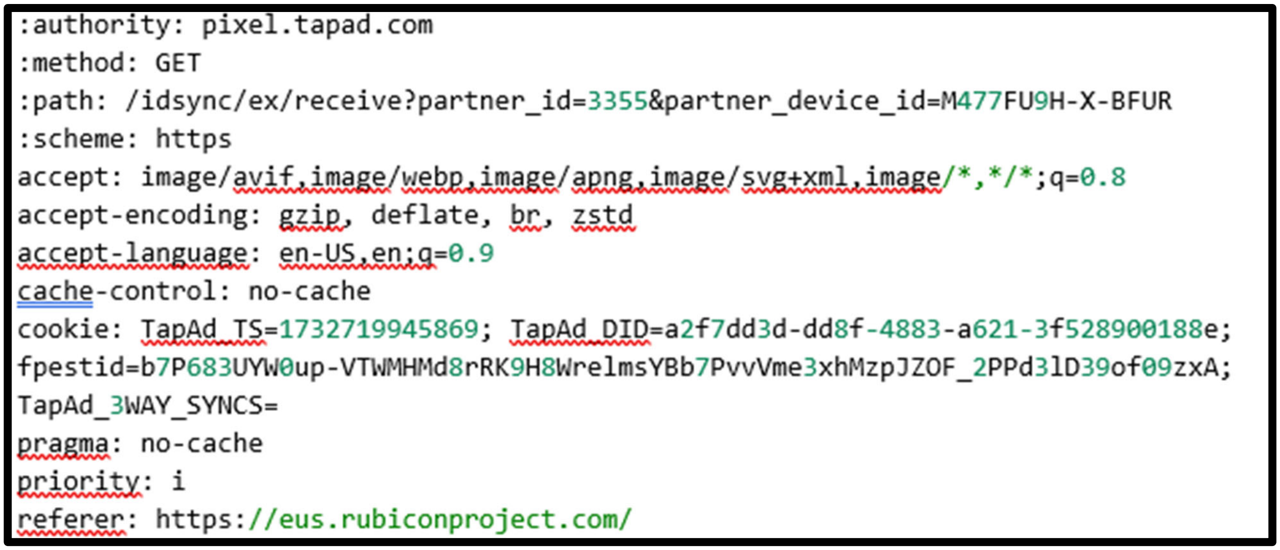


```
:authority      match.adsrvr.org
:scheme         https
:path
/track/cmf/generic?ttd_pid=tapad&ttd_tpi=1&ttd_puid=8a84a37a-c08a-4333-a36e-81a664698bf0%2
52C%252C&gdpr=0&gdpr_consent=
```

59. Once one of the pixels offered by Tapad is called to the website by a Partner Pixel, Tapad collects information automatically as users access websites and mobile applications. The below excerpt of the traffic from the Mindbloom website is illustrative, where a Tapad pixel has been called to the Zillow website by the Rubicon Partner Pixel (*see* Factual Allegations § III.E, *infra*):

//

//



```
:authority: pixel.tapad.com
:method: GET
:path: /idsync/ex/receive?partner_id=3355&partner_device_id=M477FU9H-X-BFUR
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cache-control: no-cache
cookie: TapAd_TS=1732719945869; TapAd_DID=a2f7dd3d-dd8f-4883-a621-3f528900188e;
fpestid=b7P683UYW0up-VTWMHMd8rRK9H8WrelmsYBb7PvvVme3xhMzpJZOF_2PPd3lD39of09zxA;
TapAd_3WAY_SYNCS=
pragma: no-cache
priority: i
referer: https://eus.rubiconproject.com/
```

60. Specifically, Tapad collects information used to identify individuals across the Internet including, but not limited to, cookies, IP addresses, email addresses, HTTP headers that specify information such as type of browser, device and operating system information, location information, and other unique identifiers associated with web addresses.[35] In addition, Tapad collects information regarding the users' activity on the websites and communications with the websites in the form of full-string URLs and button click events. Finally, Tapad is able to pair this information to any it has otherwise collected about the user and has compiled into a profile of the user that either Tapad or Experian maintains, as alleged below.

61. All of the above information is used to identify individuals and track their activity, but persistent identifiers and URL information play particular roles in the Tapad surveillance apparatus.

### *2. Persistent Identifiers*

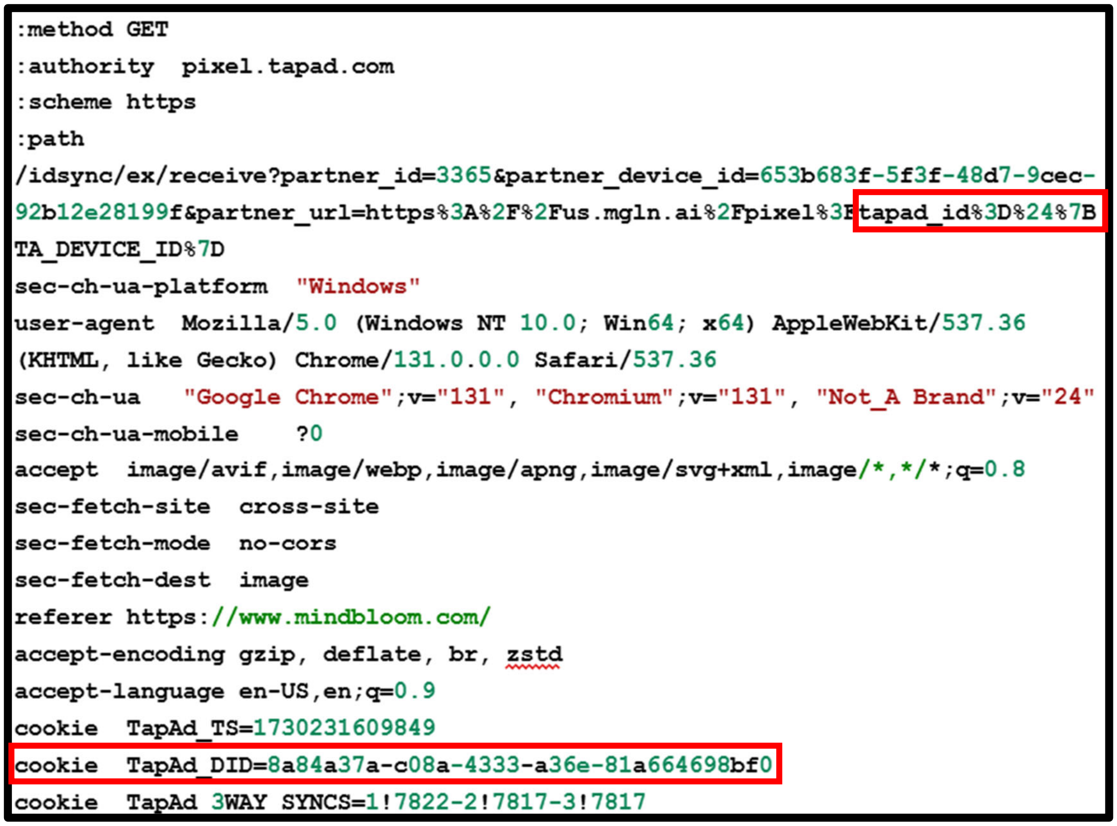
62. One way Tapad tracks individuals across multiple websites is through the use of persistent identifiers. As the name suggests, persistent identifiers are identifying information that follows an Internet user from one website or app to another. Tapad uses these identifiers to confirm that using a particular website is the same person identified by Tapad on another website.

[35] https://www.Tapad.com/global-privacy-notice (last visited Dec. 23, 2024).

63. One form of persistent identifier is a browser "cookie." "Cookies are bits of data that are sent to and from your browser to identify you. When you open a website, your browser sends a piece of data to the web server hosting that website."[36]

64. When a Tapad pixel is called onto a website, it automatically downloads a cookie onto the browser of the person visiting the website. Tapad then links a proprietary ID number to the cookie and the individual with the cookie.

65. **In other words, Tapad effectively "stamps" each cookie with its own identifier to better enable it to track individuals across the Internet:**



```
:method GET
:authority  pixel.tapad.com
:scheme https
:path
/idsync/ex/receive?partner_id=3365&partner_device_id=653b683f-5f3f-48d7-9cec-
92b12e28199f&partner_url=https%3A%2F%2Fus.mgln.ai%2Fpixel%3Ftapad_id%3D%24%7B
TA_DEVICE_ID%7D
sec-ch-ua-platform  "Windows"
user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
sec-ch-ua   "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile    ?0
accept  image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
sec-fetch-site  cross-site
sec-fetch-mode  no-cors
sec-fetch-dest  image
referer https://www.mindbloom.com/
accept-encoding gzip, deflate, br, zstd
accept-language en-US,en;q=0.9
cookie  TapAd_TS=1730231609849
cookie  TapAd_DID=8a84a37a-c08a-4333-a36e-81a664698bf0
cookie  TapAd 3WAY SYNCS=1!7822-2!7817-3!7817
```

66. After the cookie is loaded onto a person's browser, each time that person visits a website where a Tapad pixel is called, Tapad uses the cookie to identify the website visitor as the same person who visited previous websites with the same cookie installed on their browser. As such, Tapad is able to track each individual internet user across multiple sites to create a more detailed profile on that person's beliefs, interests, and habits.

[36] https://www.microsoft.com/en-us/edge/learning-center/what-are-cookies?form=MA13I2 (last visited Dec. 23, 2024).

67. This information is cross-referenced with other information collected by Tapad and Experian to specifically identify the individual using the device and to add this web-activity information to a larger profile on the individual in order to sell their profile for targeted advertising.

### a. IP Addresses

68. IP addresses are another common persistent identifier.

69. An IP address is a unique set of numbers assigned to a device on a network, which is typically expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). The traditional format of IP addresses is called IPv4, and it has a finite amount of combinations and thus is limited to approximately 4.3 billion addresses. Because this proved to be insufficient as the Internet grew, IPv6 was introduced. IPv6 offers a vastly larger address space with 340 undecillion possible addresses. While IPv6 adoption has been increasing, many networks still rely on IPv4.[37]

70. Much like a telephone number, an IP address guides or routes an intentional communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential for identifying a device on the internet or within a local network, facilitating smooth communication between devices.

71. IP addresses are not freely accessible. If an individual is not actively sending data packets out, their IP address remains private and is not broadcast to the wider internet.

72. IP addresses can be used to determine the approximate physical location of a device. For example, services like iplocation.io use databases that map IP addresses to geographic areas—often providing information about the country, city, approximate latitude and longitude coordinates, or even the internet service provider associated with the public IP.[38] Thus, knowing a user's public IP address—and therefore geographical location—"provide[s] a level of specificity previously unfound in marketing."[39]

[37] *See, e.g.*, https://www.cloudflare.com/learning/network-layer/internet-protocol/ (last visited Dec. 23, 2024); https://netbeez.net/blog/rfc1918/ (last visited Dec. 23, 2024).

[38] https://iplocation.io/ (last visited Dec. 23, 2024).

[39] *IP Targeting: Understanding This Essential Marketing Tool*, AccuData (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

73. An IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[40] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests."[41] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[42] because "[c]ompanies can use an IP address … to personally identify individuals."[43]

74. In fact, an IP address is a common identifier used for "geomarketing," which is "the practice of using location data to identify and serve marketing messages to a highly-targeted audience. Essentially, geomarketing allows [websites] to better serve [their] audience by giving [them] an inside look into where they are, where they have been, and what kinds of products or services will appeal to their needs."[44] For example, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.[45]

75. "IP targeting is a highly effective digital advertising technique that allows you to deliver ads to specific physical addresses based on their internet protocol (IP) address. IP targeting technology works by matching physical addresses to IP addresses, allowing advertisers to serve ads to specific households or businesses based on their location."[46]

[40] *Location-Based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/.

[41] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert williams-z7bhf.

[42] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[43] Trey Titone, *The Future Of IP Address As An Advertising Identifier*, AD TECH EXPLAINED (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.

[44] *See, e.g.*, *The Essential Guide to Geomarketing: Strategies, Tips & More*, DEEP SYNC (Nov. 20, 2023), https://deepsync.com/geomarketing/.

[45] *See, e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns.

[46] *IP Targeting*, SAVANT DSP, https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB.

76. "IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This means that advertisers can deliver highly targeted ads to specific households or businesses, rather than relying on more general demographics or behavioral data."[47]

77. In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's IP address because it "can be more cost-effective than other forms of advertising."[48] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[49]

78. In addition, "IP address targeting can help businesses to improve their overall marketing strategy."[50] "By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts."[51]

79. Putting IP addresses in the hands of a data broker like Tapad is particularly invasive, as the NATO report noted:

> [a] data broker may receive information about a[] [website] user, including his … IP address. The user then opens the [website] while his phone is connected to his home Wi-Fi network. When this happens, the data broker can use the IP address of the home network to identify the user's home, and append this to the unique profile it is compiling about the user. If the user has a computer connected to the same network, this computer will have the same IP address. The data broker can then use the IP address to connect the computer to the same user, and identify that user when their IP address makes requests on other publisher pages within their ad network. Now the data broker knows that the same individual is using both the phone and the computer, which allows it to track behaviour across devices and target the user and their devices with ads on different networks.[52]

//

//

//

//

[47] *Id.*

[48] Williams, https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] TWETMAN & BERGMANIS-KORATS, *supra* at 11.

80. For these reasons, under Europe's General Data Protection Regulation, IP addresses are considered "personal data, as they can potentially be used to identify an individual."[53]

### b. <u>Universal Resource Locator</u>

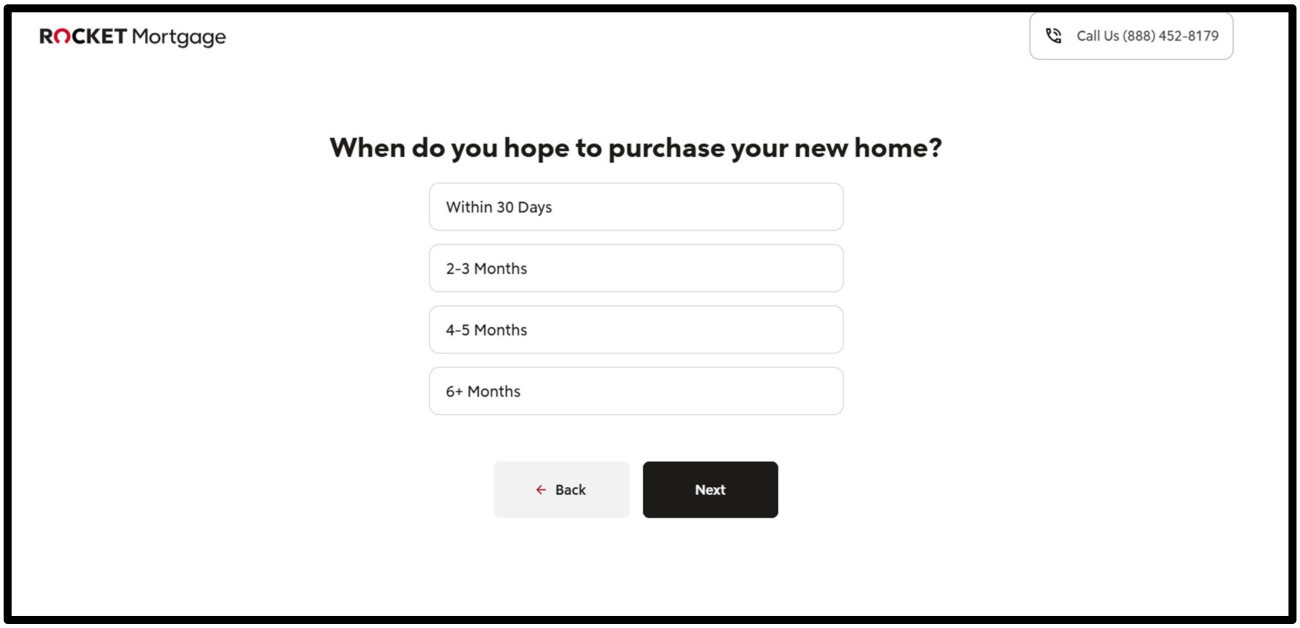
81. In addition to collecting a myriad of identifiers, the Tapad pixels collect the Universal Resource Locator (URL) of the webpages visited by each individual.

82. Sometimes known as a "web address," the URL is the name of the webpage as displayed in the address bar of a browser.

83. Each page on a website has its own individual URL, allowing pixels with access to the URL to see which pages of a website a particular internet user visited.

84. All URLs identify the pages of each page of a website an internet user visited, but some—depending on the design of the website—also disclose the contents of information entered onto a webpage. These URLs are known as full-string descriptive URLs.

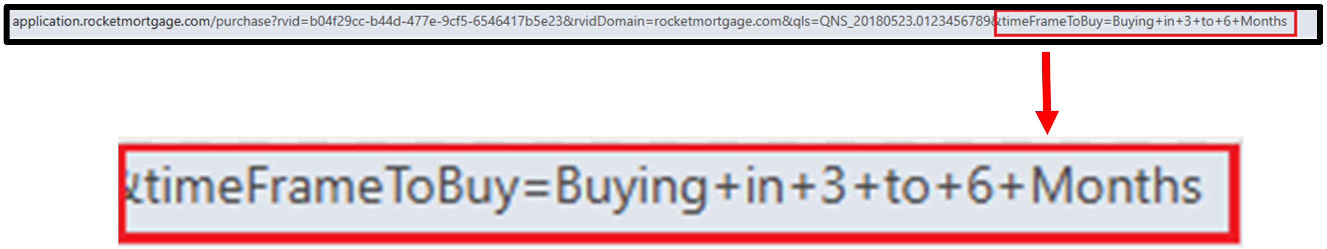
85. For example, when applying for a loan on the Rocket Mortgage website, the user answers a question about when they plan to purchase a home.



When do you hope to purchase your new home?

[53] Is an IP Address Personal Data?, Convesio, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/; *see also* What Is Personal Data?, European Commission, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

86. When the user clicks the "next" button, the URL for the next page contains the answer to this question:



application.rocketmortgage.com/purchase?rvid=b04f29cc-b44d-477e-9cf5-6546417b5e23&rvidDomain=rocketmortgage.com&qls=QNS_20180523.0123456789&timeFrameToBuy=Buying+in+3+to+6+Months

&timeFrameToBuy=Buying+in+3+to+6+Months

87. As such, any pixel that intercepts the URL on this page also intercepts the content of the users' communications with Rocket Mortgage about when they plan to purchase a home. This process works similarly on other websites.

88. The Tapad pixels collect both types of URLs and any information that can be gleaned or inferred from those URLs are added to the profiles that Defendants have for that particular user.

### c. <u>Mobile Advertising Identifiers</u>

89. Tapad employs similar methods to track individuals using mobile apps on Android and iOS devices.

90. Tapad owns and operates multiple "software development kits" (SDKs), pieces of code that work independently or with "application programming interfcaes" (APIs) and are loaded into mobile apps and can track users' activity on certain apps.[54]

91. An SDK is a "set of tools for developers that offers building blocks for the creation of an application instead of developers starting from scratch … For example, Google Analytics provides an SDK that gives insight into user behavior, engagement, and cross-network attribution."[55]

92. An API "acts an intermediary layer that processes data transfer between systems, letting companies open their application data and functionality to external third-party developers [and] business partners."[56] An API can "work[] as a standalone solution or included within an SDK

[54] https://www.ibm.com/blog/sdk-vs-api/ ("SDK" stands for software development kit and "is a set of software-building tools for a specific program," while "API" stands for application programming interface) (last visited Dec. 23, 2024). Plaintiffs will refer to both collectively as the "Tapad SDKs" to avoid any confusion.

[55] API vs. SDK: The Difference Explained (With Examples), https://getstream.io/glossary/api-vs-sdk/.

[56] IBM, *What is an API?*, available https://www.ibm.com/topics/api.

… [A]n SDK often contains at least one API."[57] APIs "enable[] companies to open up their applications' [or websites'] data and functionality to external third-party developers, business partners, and internal departments within their companies."[58]

93. Similar to the pixels on web browsers, the Tapad SDKs are called by other SDKs when a user accesses a particular app.

94. The Tapad SDKs track the types of user information Defendants obtain through the Tapad pixels including, but not limited to, users': location information, email addresses, device and advertising identifiers, and usage of the particular app being accessed.

95. In addition to its own ID tracking, Tapad collects advertising identifiers that are designed to track the app activity of individual users across different apps. Two of the most prominent are AAIDs (for Android devices) and IDFAs (for iOS devices) (collectively, "Mobile Advertising IDs" or "MAIDs").

96. An AAID is a unique string of numbers which attaches to a device. As the name implies, an AAID is sent to advertisers and other third parties so they can track user activity across multiple mobile applications.[59] So, for example, if a third party collects AAIDs from two separate mobile applications, it can track, cross-correlate, and aggregate a user's activity on both apps.

97. Although technically resettable, an AAID is a persistent identifier because virtually no one knows about AAIDs and, correspondingly, virtually no one resets that identifier. The fact that the use and disclosure of AAIDs is so ubiquitous evinces an understanding on the part of Defendants, Google, and others in the field that they are almost never manually reset by users (or else an AAID would be of no use to advertisers). Byron Tau, MEANS OF CONTROL: HOW THE HIDDEN ALLIANCE OF TECH AND GOVERNMENT IS CREATING A NEW AMERICAN SURVEILLANCE STATE at 175 (2024) ("Like me, most people had no idea about the 'Limit Ad Tracking' menu on their iPhones or

[57] SDK VS. API: WHAT'S THE DIFFERENCE?, IBM (July 13, 2011), https://www.ibm.com/blog/sdk-vs-api/ ("SDK" stands for software development kit and "is a set of software-building tools for a specific program," while "API" stands for application programming interface).

[58] APPLICATION PROGRAMMING INTERFACE (API), https://www.ibm.com/cloud/learn/api.

[59] https://support.google.com/googleplay/android-developer/answer/6048248 (last visited Dec. 23, 2024).

the AAID that Google had given even Android devices. Many still don't."); *see also Louth v. NFL Enterprises LLC*, 2022 WL 4130866, at *3 (D.R.I. Sept. 12, 2022) ("While AAID are resettable by users, the plaintiff plausibly alleges that AAID is a persistent identifier because virtually no one knows about AAIDs and, correspondingly, virtually no one resets their AAID.") (cleaned up).

98. Using publicly available resources, an AAID can track a user's movements, habits, and activity on mobile applications.[60] Put together, the AAID serves as "the passport for aggregating all of the data about a user in one place."[61]

99. Because an AAID creates a record of user activity, this data can create inferences about an individual, like a person's political or religious affiliations, sexuality, or general reading and viewing preferences. These inferences, combined with publicly available tools, make AAIDs an identifier that sufficiently permits an ordinary person to identify a specific individual.

100. Similarly, an "Identifier for Advertisers, or IDFA for short, is a unique, random identifier (device ID) that Apple assigns to every iOS device. An IDFA would be the equivalent of a web cookie, in the sense that it enables advertisers to monitor users' engagement with their ads, and keep track of their post-install activity."[62]

101. As with the Tapad cookie and AAID, Tapad's collection of IDFAs allows Tapad to track iOS users' activity across the various apps they use. Like the AAID, this data can create inferences about an individual, such as a person's political or religious affiliations, sexuality, or general reading and viewing preferences. These inferences, combined with publicly available tools, sufficiently permits even an ordinary person to identify a specific individual with the IDFA.

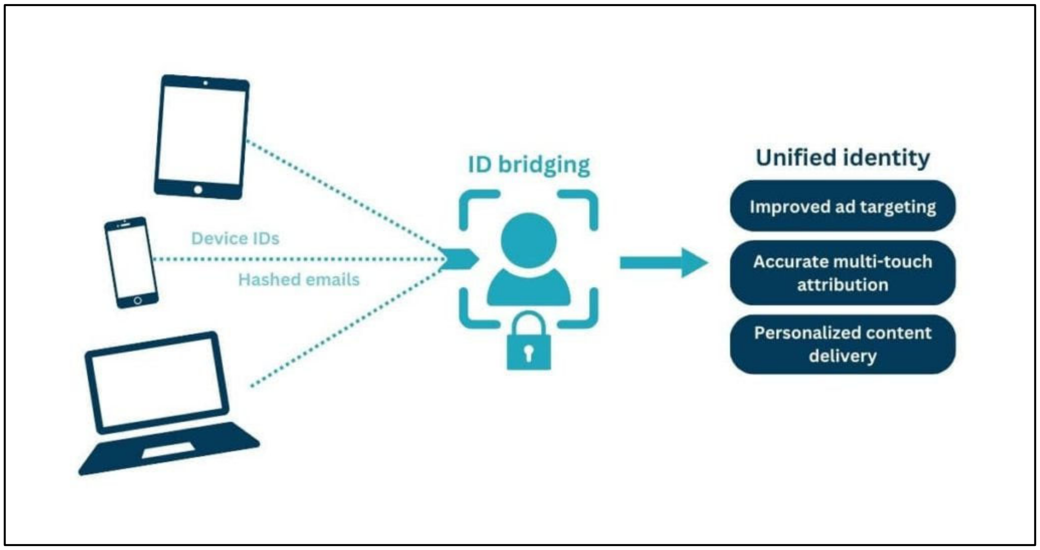
102. Regardless of whether these IDs are supposed to be anonymous, MAIDs are often combined with other identifiers to identify users in what is known as ID Bridging. "ID Bridging" is the process of "piecing together different bits of information about" a user "to confidently infer that

[60] https://www.huffingtonpost.co.uk/entry/using-just-1000-worth-of-mobile-adverts-you-can-effectively-track-anyone_uk_59e87ccbe4b0d0e4fe6d6be5 (last visited Dec. 23, 2024).

[61] https://digitalwatchdog.org/trend-report-apps-oversharing-your-advertising-id/ (last visited Dec. 23, 2024).

[62] https://www.appsflyer.com/glossary/idfa/#:~:text=Identifier%20for%20Advertisers%2C%20or%20IDFA,of%20their%20post%2Dinstall%20activity (last visited Dec. 23, 2024).

it is the same individual accessing a publisher's site or sites from various devices or browsers."[63] That is, users can be identified and tracked by "bridging" (or linking) their MAIDs to other sources, such as e-mail addresses, geolocation, or phone numbers.



103. ID Bridging "has long been the foundation of programmatic advertising,"[64] which is the process by which companies "use [] advertising technology to buy and sell digital ads" by "serv[ing] up relevant ad impressions to audiences through automated steps, in less than a second."[65] It entails a "unique identifier[] assigned to individual devices," including "Google's Advertising ID," personal information like geolocation and e-amil address, and "cross-platform linkage."[66]

104. ID Bridging is a money-making machine for advertisers and app developers. On the advertiser side, ID Bridging "increase the chances of an ad buying platform finding their inventory to be addressable and, therefore, maximizes their 'ad yields.'" And on the app developer side,

[63] Kayleigh Barber, *WTF Is The Difference Between Id Bridging And Id Spoofing?*, DIGIDAY (July 8, 2024, https://digiday.com/media/wtf-is-the-difference-between-id-bridging-and-id-spoofing/.

[64] https://www.adexchanger.com/data-driven-thinking/how-can-id-bridging-the-foundation-of-our-space-suddenly-be-a-bad-thing/.

[65] PROGRAMMATIC ADVERTISING, https://advertising.amazon.com/blog/programmatic-advertising#.

[66] Anete Jodzevica, I*D Bridging: The Privacy-First Future of Audience Targeting*, SETUPAD (Nov. 15, 2024), https://setupad.com/blog/id-bridging/. Ironically, the example given in this article is a "hashed e-mail," where the e-mail Defendant collected in this example is not hashed.

"publishers can boost revenue from direct-sold campaigns by offering advertisers access to more defined and valuable audiences."[67]

105. In other words, advertisers will be able to find users that are more directly and likely interested in what is being sold by having access to significantly more information. And app users' information will be more valuable (and therefore, bring in more money to app developers) because it is combined with a plethora of other information from various sources.

106. Many companies (*e.g.*, data brokers, identity graph providers), publicly advertise their ability to conduct such bridging. And Experian itself has touted the benefits of ID Bridging, noting that "ID bridging is the supply-side practice of connecting the dots between available signals, that were generated in a way that is not the expected default behavior, to understand a user's identity and communicate it to prospective buyers. It enables the supply-side to extend user identification beyond the scope of one browser or device."[68]

107. Yet, while those within the ID Bridging industry describe it as privacy-protective, it is anything but. As courts have noted, the "ability to amass vast amounts of personal data for the purpose of identifying individuals and aggregating their many identifiers" creates "dossiers which can be used to further invade [users] privacy by allowing third parties to learn intimate details of [users'] lives, and target them for advertising, political, and other purposes, ultimately harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them." *Katz-Lacabe v. Oracle Am., Inc.*, 688 F. Supp. 3d 928, 940 (N.D. Cal. 2023) (cleaned up).

108. In February 2019, Oracle published a paper entitled "Google's Shadow Profile: A Dossier of Consumers Online and Real World Life," part of which provides as accurate a description of Google's services (and Oracle's, ironically) as Defendants':

[67] Bennett Crumbling, *What Is 'ID Bridging' And How Publishers Use It To Grow Direct And Programmatic Revenue?*, OPTABLE (Aug. 22, 2024. https://www.optable.co/blog/what-is-id-bridging.

[68] Budi Tanzi, *New OpenRTB Specs Ensure Identity Resolution Can Be Done Transparently With Trusted Partners*, EXPERIAN (Dec. 18, 2024), https://www.experian.com/blogs/marketing-forward/new-openrtb-specs-ensure-identity-resolution-can-be-done-transparently-with-trusted-partners/.

> a consumer's "shadow profile" [is a] massive, largely hidden dataset[] of online and offline activities. This information is collected through an extensive web of … services, which is difficult, if not impossible to avoid. It is largely collected invisibly and without consumer consent. Processed by algorithms and artificial intelligence, this data reveals an intimate picture of a specific consumer's movements, socio-economics, demographics, "likes", activities and more. It may or may not be associated with a specific users' name, but the specificity of this information defines the individual in such detail that a name is unnecessary.[69]

109. In other words, ID Bridging is dangerous because of the sheer expanse of information being compiled by companies like Defendants without the knowledge or consent of users, all of which is being done for pecuniary gain.

### d. Other Identifiers

110. In addition to the methods described above, which are explicitly designed to track individuals across different devices and apps, Tapad collects other identifying information that allows it to determine whether the same individual is visiting multiple websites or using multiple apps where Tapad technology is called to or installed directly.

111. One method is through collecting e-mail addresses. The logic of this is straightforward. If Tapad collects the same e-mail address from two different site visits, it can determine with almost total accuracy that the sites are both being visited by the same person. The same is true of devices. If the same e-mail address is captured on two different devices, it is very likely those devices are used by the same individual.

112. Location information functions in a similar manner. If multiple websites or apps are visited from the same location, the pool of potential individuals who are accessing the website or app is narrowed considerably immediately and can be narrowed to a pinpoint over time.

113. HTTP requests, when intercepted by Tapad, collect device information that can also identify whether the same user is visiting multiple sites or apps, and can distinguish between the devices being used by a particular person. With every visit, and every subsequent HTTP request, the device information will be identical in each.

[69] GOOGLE'S SHADOW PROFILE: A DOSSIER OF CONSUMERS ONLINE AND REAL WORLD LIFE at 1 (Feb. 2019), https://tinyurl.com/2mtuh7vf.

### *3. Identity Resolution*

114. In addition to its own tracking of individuals across the internet, Tapad sells its tracking services to other advertisers who own and operate pixels through a process known as identity resolution.

115. Identity resolution is the technology marketing term for the process of data tracking described above. As Experian describes it:

> [i]dentity resolution matches fragmented identifiers to a single profile. This creates a unified, cross-channel view of a consumer that helps marketers understand a customer's demographics, lifestyle, interests, and where and how they engage with your brand. Identity resolution improves campaign targeting and enables marketers to deliver personalized marketing messages.[70]

116. In plain language, identity resolution is the culmination of Tapad's tracking, where it assigns a Tapad ID number to an individual so that the individual is attached to a record of their web and app activity for the purpose of targeted advertising.

117. Once sufficient data has been collected on an individual, Defendants monetize the individual's data in a number of ways. One way is to provide individuals' identities and web browsing information to the companies operating the Partner Pixels to assist with those companies' collection of internet users' data.

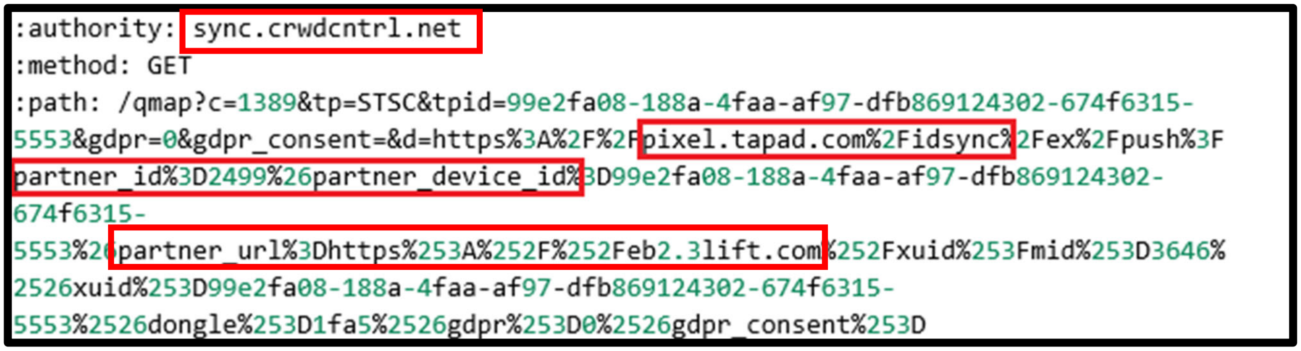
118. When a Partner Pixel is loaded onto a website and calls a Tapad pixel onto the website, the Tapad pixel (in addition to the independent tracking described above) interacts with the pixel that called Tapad onto the site. Specifically, Tapad provides the Tapad ID number to each of the pixels it interacts with and allows those pixels to access the information associated with each individual.

119. In a particular privacy-egregious example of this process from the Zillow website (Factual Allegations § III.E, *infra*), the "Crowd Control" Partner Pixel[71]—which is operated by *yet*

[70] https://www.experian.com/marketing/consumer-sync/identity-resolution (last visited Dec. 23, 2024).

[71] LOTAME CROWD CONTROL, CONDUIT, https://app.getconduit.app/web/integration/lotame-crowd-control/.

*another* data broker called Lotame[72]—is calling a Tapad pixel, and thereby connecting Lotame's own immense repository of user profiles[73] and information with Tapad's. On top of this, all of this information is *also* then being connected with and provided to the TripleLift (or 3Lift) pixel, a Supply Side Platform,[74] meaning this transmission is part of the real-time bidding process. *See* Factual Allegations § I.B, *supra*.



```
:authority: sync.crwdcntrl.net
:method: GET
:path: /qmap?c=1389&tp=STSC&tpid=99e2fa08-188a-4faa-af97-dfb869124302-674f6315-
5553&gdpr=0&gdpr_consent=&d=https%3A%2F%2Fpixel.tapad.com%2Fidsync%2Fex%2Fpush%3F
partner_id%3D2499%26partner_device_id%3D99e2fa08-188a-4faa-af97-dfb869124302-
674f6315-
5553%26partner_url%3Dhttps%253A%252F%252Feb2.3lift.com%252Fxuid%253Fmid%253D3646%
2526xuid%253D99e2fa08-188a-4faa-af97-dfb869124302-674f6315-
5553%2526dongle%253D1fa5%2526gdpr%253D0%2526gdpr_consent%253D
```

120. So, in this example, by calling the Tapad pixel, the user profiles of no less than *three* data brokers (Tapad, Experian, and Lotame) are being linked and combined together, sent to any number of advertisers for bidding and targeted advertising, and enriching Defendants, the other technology companies involved, and Zillow alike while trampling consumer privacy in the process. And transmissions similar to this one are happening across all of the websites and apps that the Tapad pixels are being called to.

121. With respect to the delivery of targeted advertisements on websites, Tapad's ID syncing makes the entire real-time-bidding process possible by identifying the individual visiting the site and providing information about their web activity and interests. This creates the basis for hyper-targeted advertising related to that activity and those interests to be served. This ultimately benefits the website or app operator, as it makes their userbase more valuable because said users have been further identified and linked to other activity via the Tapad pixels.

[72] DATA BROKER REGISTRATION FOR LOTAME SOLUTIONS, INC., https://oag.ca.gov/data-broker/registration/186954.

[73] PANORAMA GRAPH, https://www.lotame.com/panorama-identity-graph/ (noting Lotame "unlocks addressability to 1.3 billion users with global coverage").

[74] TRIPLELIFT, https://triplelift.com/.

122. For these processes to happen, Tapad must necessarily share the information it collects on individual internet users with its partners.

123. The identity resolution service aids in the wiretapping and surveillance conducted by the Pixel Partners.

124. As part of their investigation, Plaintiffs' counsel conducted testing on several websites to provide a sample of the widespread tracking and wiretapping of, and targeted advertising to, millions of Americans by Tapad. For each of the websites tested, there are hundreds or thousands of others where the same or similar information is collected. *See* Factual Allegations § III, *infra*.

125. Specifically, Plaintiffs' counsel found that each website and/or app had Partner Pixels loaded onto it, which in turn called Tapad to better enable their advertising. Each Partner Pixel would itself intercept users' communications with the website or app. Each Partner Pixel—which contracted with Defendants—would then call a Tapad pixel to aid or enable this interception. The Tapad pixel would then assign a Tapad ID to the user's activity on the website or app, which, among other things, (i) allowed for the user to be identified; (ii) link the user to information from across other websites and apps; and (iii) benefit the websites, apps, and Partner Pixels by making that user more valuable to advertisers because the user could be better targeted with relevant ads due to the extensive information Tapad collected and provided to the Partner Pixels.

### B. Experian

126. Experian is a multinational data analytics and consumer credit reporting company and one of the largest data brokers in the world.

127. As the Duke Sanford report noted, Experian "processes over 2 billion records monthly and has over 8 billion name and address combinations, with the ability to convert sensitive [] personally identifiable information data into actionable insights."[75]

128. Experian "advertises data on 95% of the U.S. population … spanning thousands of attributes." Experian does so by "ingest[ing] first-party data such as names, physical addresses, email addresses, mobile ad identifiers (MAIDs), IP addresses, and other information to link economic

[75] SHERMAN, *supra*, at 6 (cleaned up).

transactions to an Experian household ID. It advertises mobile location data on users and the ability to link information to 500 million email addresses and 275 million addressable cookies."[76]

129. In addition to collecting and aggregating credit reporting information on billions of people, Experian tracks many of those same people to sell decision analytic and marketing assistance to businesses, including individual fingerprinting and targeting for advertising.[77]

130. "[U]sing Tapad's technology as the foundation," Experian developed products that combine its "offline consumer data set (purchase behaviors, interests, lifestyle info) with online consumer data (media consumption habits and device usage) collected by Tapad.[78]

131. Tapad's products, which include detailed profiles on the web and purchase habits of nearly every American, are constantly updated by the widespread tracking of individuals across the internet.

132. Experian has access to all the data collected by the Tapad pixels and SDKs described above, including Tapad's device graph. This, however, is not the totality of Experian's data. Experian also obtains data from other surveillance projects, from third parties it contracts with to receive information, and from publicly available sources.

133. In fact, "[a]s a data broker, Experian has access to behavioral and demographic data on more than 300 million Americans across 125 million households and 2 billion devices."[79]

134. Experian combines this data into detailed profiles on individual consumers that track both intimate web activity but also use highly sophisticated technology to identify a user through various separate pieces of identifying information.

135. These profiles, which include the data continuously tracked by Tapad, are used as the basis for Experian's suite of products available to marketers.

[76] *Id.* (cleaned up).

[77] https://www.reuters.com/article/uk-facebook-privacy/facebook-cuts-ties-to-data-brokers-in-blow-to-targeted-ads-idUKKBN1H41LZ/?edition-redirect=uk (last visited Dec. 23, 2024).

[78] Vargas, *supra*, https://www.adexchanger.com/data-exchanges/how-experian-is-using-Tapad-to-build-new-id-resolution-and-analytics-products/.

[79] *Id.*

136. One such Experian product is Consumer View. "Consumer View encompasses all of Experian's services that help marketers understand audiences and consumer behavior, including audience insights and discovery, analytics and measurement and Experian's marketplace for third-party audience data sets."[80]

137. Experian boasts about the accuracy of these services, explaining how Consumer View helps marketers "identify [] customers, their values, and … gain an accurate and deeper understanding of consumers, their patterns, and their journey" through their lives and in relation to various Experian customers who are looking to increase the specificity and, ultimately, effectiveness of their advertising.[81]

138. Another product offered by Experian to marketers is Consumer Sync. Consumer Sync "combines Experian's data with marketer data sets via cross-device ID resolution and audience matching. It also scouts potential new customers using AI and machine learning to match lookalike audiences across first-party and third-party data."[82]

139. Experian, again, advertises the scope of this data, advertising that its "digital technology assets bring in 4 billion devices and 1 trillion device signals to definitively connect offline records to online identifiers."[83]

140. Experian is explicit that it combines the data it collects online through the mass deployment of Tapad, with its existing sets of offline data collected by both Experian and other parties.

141. Experian further markets its data products to sell that data to other parties who also use the data for hyper-specific marketing, advertising, and brand analytics on an individual level.

142. The purpose of this is straightforward: Experian reaps massive profits by tracking consumers with Tapad's pixels and SDKs. This necessarily involves using (and having the capability

[80] *Id.*

[81] https://www.experian.com/marketing/consumer-view (last visited Dec. 23, 2024).

[82] Vargas, *supra*, https://www.adexchanger.com/data-exchanges/how-experian-is-using-Tapad-to-build-new-id-resolution-and-analytics-products/..

[83] https://www.experian.com/marketing/consumer-sync (last visited Dec. 23, 2024).

to use) the data collected for Experian's own purposes, rather than exclusively for use regarding the individual websites where individual data points are collected.

143. Further, Experian knows that (i) it will be able to identify an individual internet user by combining Tapad data and its existing device graph, profiles including offline data, and data acquired from other parties and (ii) the parties who add data to its Consumer Sync product and other products can use the data from Tapad and triangulate the identities of individual internet users with their own data.

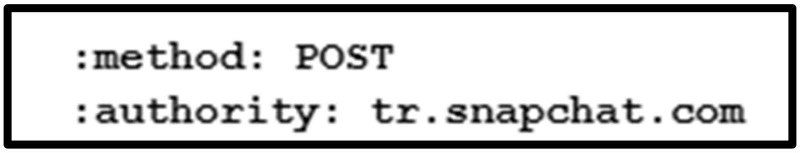
## III. DEFENDANTS' TAPAD PIXELS ARE PRESENT ON EACH OF THE SUBJECT WEBSITES

144. As demonstrated below, Defendants' Tapad Pixels are present on each of the websites visited by Plaintiffs, collect information on Plaintiffs' and Class Members' interactions with those websites, and assist the Pixel Partners in the wiretapping and surveillance of Plaintiffs and Class Members on the subject websites.

### A. GEICO

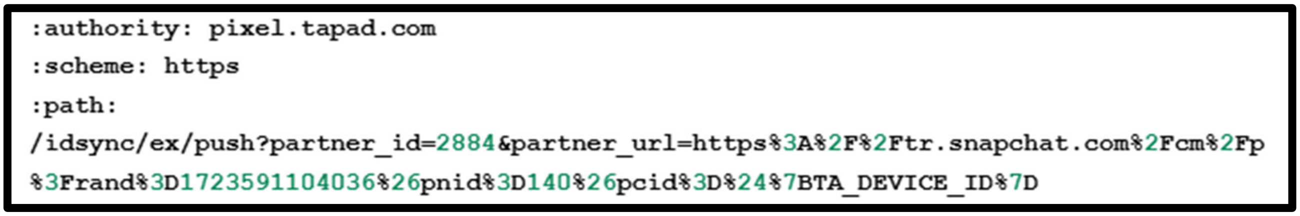
145. The website for the major insurance company, GEICO (which stands for "Government Employees Insurance Company"), allows visitors to obtain quotes for insurance.

146. Unbeknownst to website visitors, the Snap Pixel—one of the Partner Pixels owned and operated by third-party Snap, Inc. ("Snapchat")—is loaded onto the GEICO online insurance application.

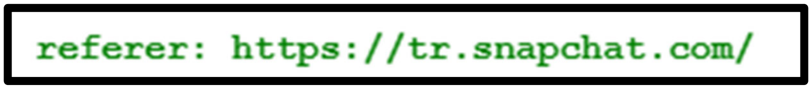


```
:method: POST
:authority: tr.snapchat.com
```

147. When a user accesses the GEICO website, the Snap Pixel automatically calls a Tapad pixel onto the website.



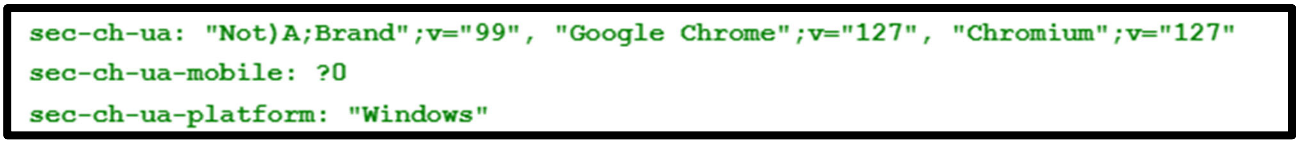
```
:authority: pixel.tapad.com
:scheme: https
:path:
/idsync/ex/push?partner_id=2884&partner_url=https%3A%2F%2Ftr.snapchat.com%2Fcm%2Fp
%3Frand%3D1723591104036%26pnid%3D140%26pcid%3D%24%7BTA_DEVICE_ID%7D
```



```
referer: https://tr.snapchat.com/
```

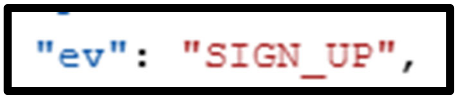
148. When called onto the GEICO website by Snapchat, Tapad provides the Tapad ID and information from its ID Graph to Snapchat so that Snapchat can identify the individual visiting the website and target that person with hyper-specific advertising related to the insurance application visited. SnapChat can also target the user with advertisements related to any other information that Defendants may possess about the user in that user's profile, which has now been connected to the Snap Pixel via the Tapad ID.

149. Tapad also collects a variety of identifiers and device information as described in detail above.



```
sec-ch-ua: "Not)A;Brand";v="99", "Google Chrome";v="127", "Chromium";v="127"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
```

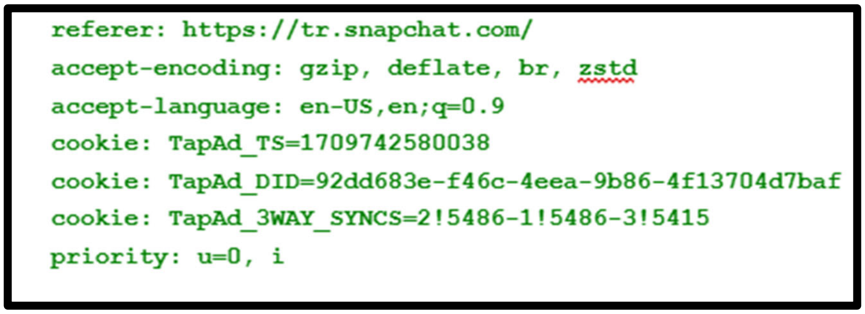
150. Tapad and Snapchat also receive information sufficient to show that the quote was requested because the "sign up" page comes after the quote request form.



```
"ev": "SIGN_UP",
```

151. Tapad then adds this information to its profile on the individual. This profile is connected to the Tapad ID assigned to the individual and added to Defendants' ID Graph, Consumer View, and Consumer Sync. This data added to an individual's profile increases its value to advertisers—who can serve ads related to insurance to the individual—and enriches GEICO—as its users are more valuable now that their information is being connected to Defendants' vast repository of information and user profiles.

152. In addition, when an internet user visits the GEICO website, Tapad loads its cookie onto the individual's browser as described above.



```
referer: https://tr.snapchat.com/
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cookie: TapAd_TS=1709742580038
cookie: TapAd_DID=92dd683e-f46c-4eea-9b86-4f13704d7baf
cookie: TapAd_3WAY_SYNCS=2!5486-1!5486-3!5415
priority: u=0, i
```

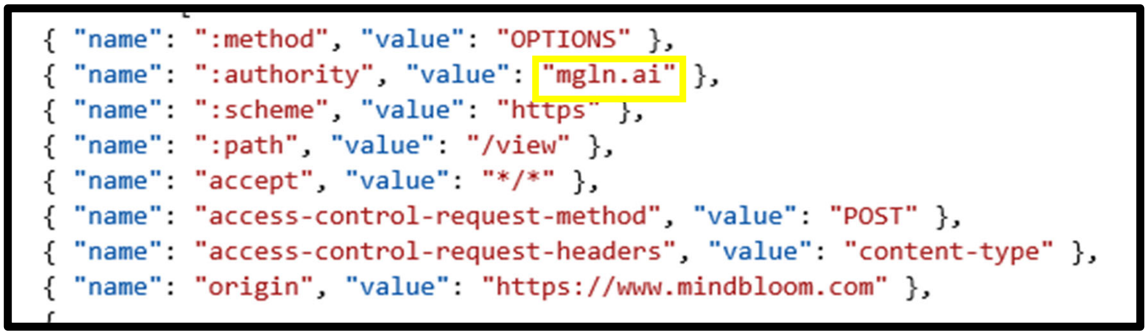
153. Tapad then tracks the future web activity of the individual and adds that information to its consumer profile and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

**B. Mindbloom**

154. Mindbloom is a medical website offering prescription plans of ketamine therapy for purchase as a treatment for certain mental health conditions, including depression and anxiety.

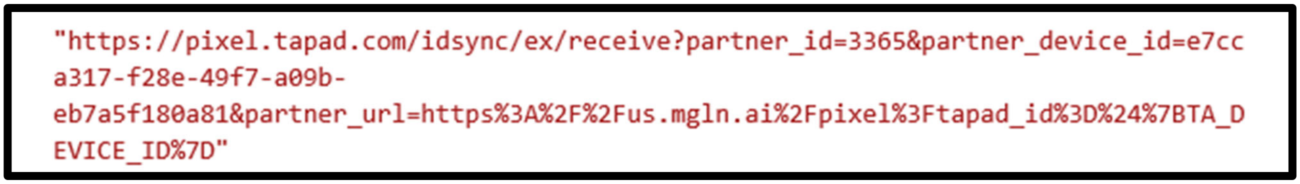
155. Patients seeking these treatments answer intake questions on the website and can make their purchase if they are approved for a prescription.

156. One of the Partner Pixels owned by a third-party company, Magellan AI (the "Magellan Pixel"), is loaded onto all pages of the Mindbloom website.



```
{ "name": ":method", "value": "OPTIONS" },
{ "name": ":authority", "value": "mgln.ai" },
{ "name": ":scheme", "value": "https" },
{ "name": ":path", "value": "/view" },
{ "name": "accept", "value": "*/*" },
{ "name": "access-control-request-method", "value": "POST" },
{ "name": "access-control-request-headers", "value": "content-type" },
{ "name": "origin", "value": "https://www.mindbloom.com" },
{
```

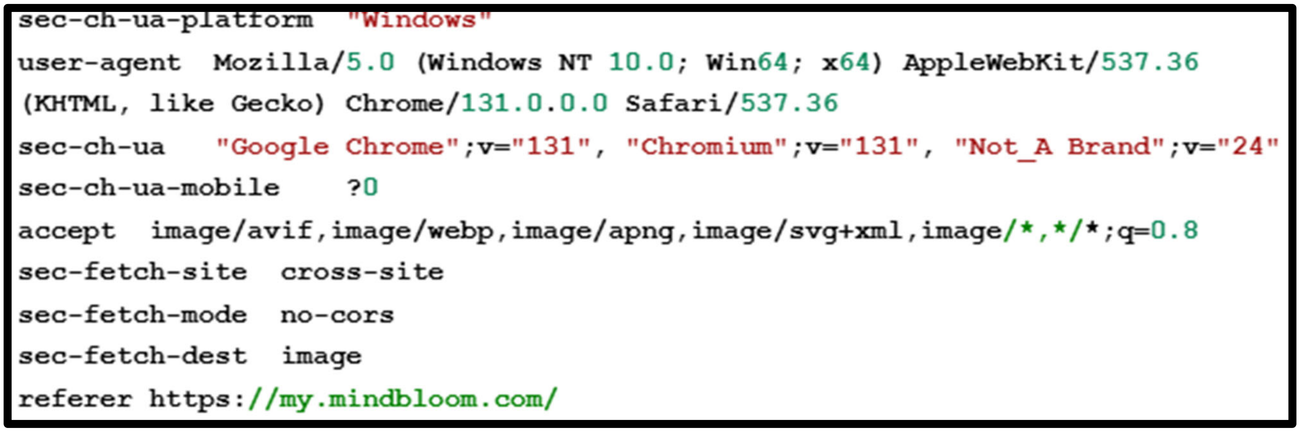
157. When an internet user navigates the Mindbloom webite, the Magellan Pixel automatically calls a Tapad pixel onto the website.



```
"https://pixel.tapad.com/idsync/ex/receive?partner_id=3365&partner_device_id=e7cc
a317-f28e-49f7-a09b-
eb7a5f180a81&partner_url=https%3A%2F%2Fus.mgln.ai%2Fpixel%3Ftapad_id%3D%24%7BTA_D
EVICE_ID%7D"
```

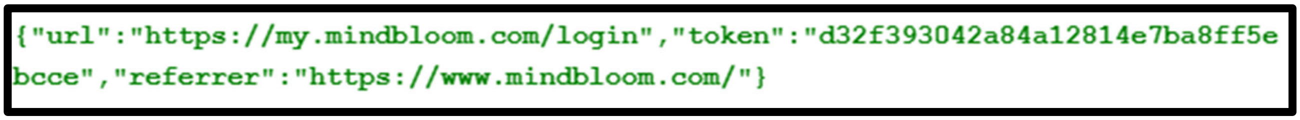
158. When called on to the site by Magellan AI, Tapad provides the Tapad ID and information from its ID Graph to Magellan AI so that Magellan AI can identify the individual visiting the website and target that person with hyper-specific advertising related to their seeking medical treatment on the Mindbloom website. Magellan AI can also target the user with advertisements related to any other information that Defendants may possess about the user in that user's profile, which has now been connected to the Magellan AI Pixel via the Tapad ID.

159. Tapad also collects a variety of identifiers and device information in the manner described in detail above.



```
sec-ch-ua-platform  "Windows"
user-agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
sec-ch-ua   "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile    ?0
accept  image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
sec-fetch-site  cross-site
sec-fetch-mode  no-cors
sec-fetch-dest  image
referer https://my.mindbloom.com/
```

160. In addition, both Magellan and Tapad, who now both have access to the individual's identity, receive URL information identifying that the individual visited the Mindbloom website.

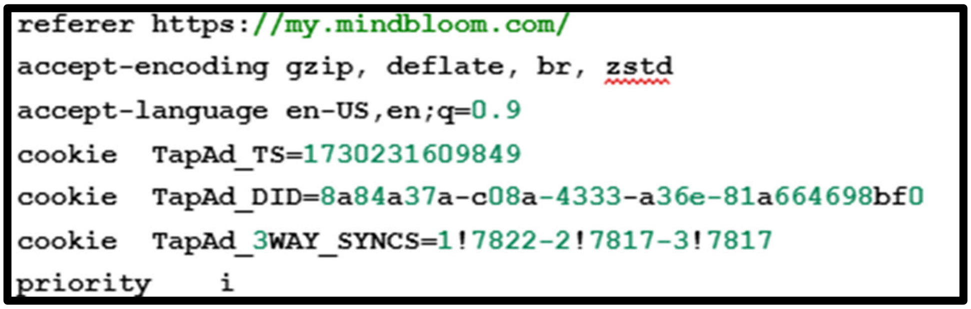


```
{"url":"https://my.mindbloom.com/login","token":"d32f393042a84a12814e7ba8ff5e
bcce","referrer":"https://www.mindbloom.com/"}
```

161. Because Mindbloom only provides ketamine therapy and related services, Tapad intercepts information sufficient to conclude that the individual it is tracking is seeking ketamine therapy (*i.e.*, information about the individual's confidential medical treatment) and that the individual suffers from a narrow range of mental health conditions for which ketamine therapy is a treatment (confidential information about an individual's medical condition).

162. Tapad then adds this information to its profile on the individual. This profile is connected to the Tapad ID assigned to the individual and added to Defendants' ID Graph, Consumer View and Consumer Sync described herein. This data added to an individual's profile increases its value to advertisers—who can serve ads related to mental health treatment to the individual—and enriches Mindbloom —as its users are more valuable now that their information is being connected to Defendants' vast repository of information and user profiles.

163. In addition, when an internet user visits the Mindbloom website, Tapad loads its cookies onto the individual's browser as described above.



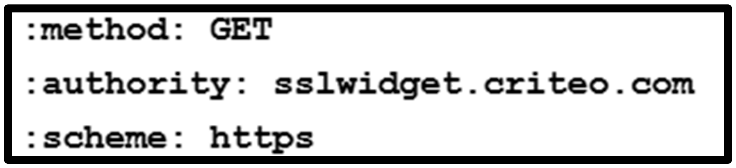
```
referer https://my.mindbloom.com/
accept-encoding gzip, deflate, br, zstd
accept-language en-US,en;q=0.9
cookie  TapAd_TS=1730231609849
cookie  TapAd_DID=8a84a37a-c08a-4333-a36e-81a664698bf0
cookie  TapAd_3WAY_SYNCS=1!7822-2!7817-3!7817
priority    i
```

164. Tapad then tracks the future web activity of the individual and adds that information to its consumer profile and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

### C. Loan Depot

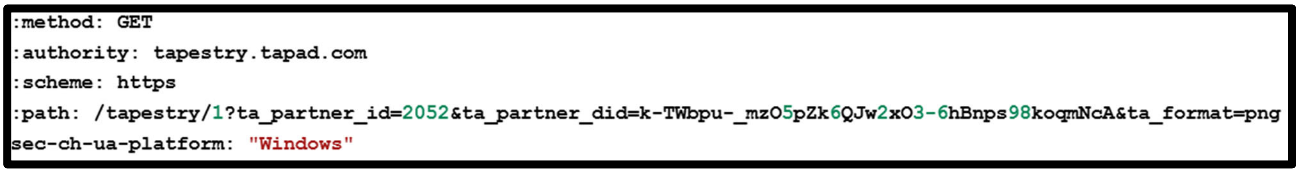
165. Loan Depot offers home loans and refinancing. The loan applications can be submitted on its website, loandepot.com.

166. Unbeknownst to website visitors, the Criteo Pixel is loaded onto the Loan Depot website.



```
:method: GET
:authority: sslwidget.criteo.com
:scheme: https
```

167. When a user accesses the Loan Depot website, the Criteo Pixel automatically calls a Tapad pixel onto the website.

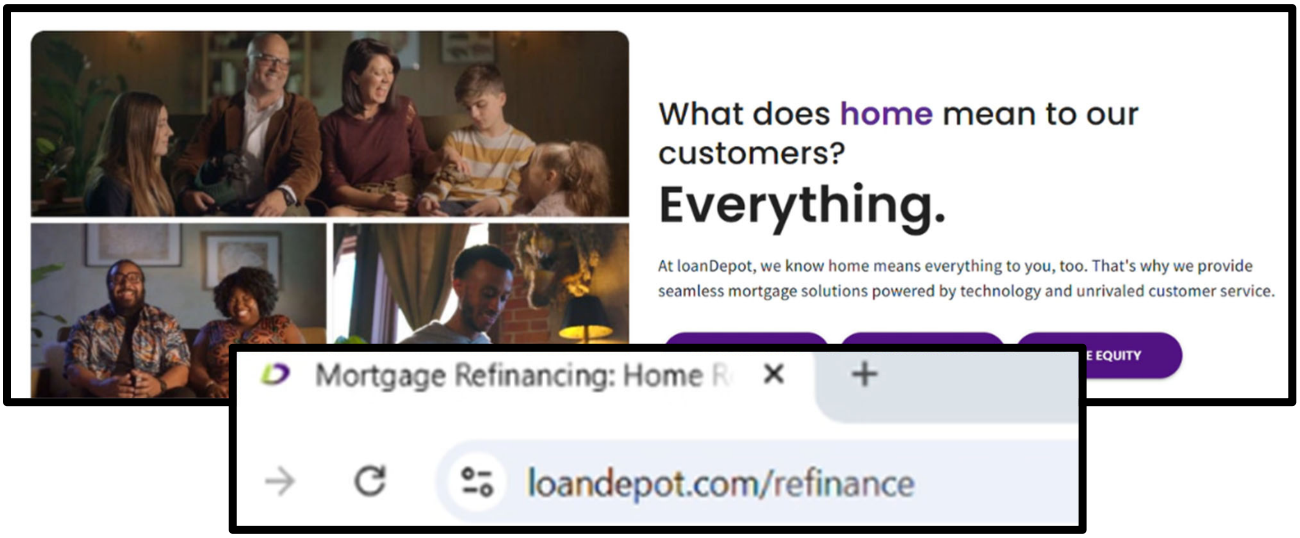


```
:method: GET
:authority: tapestry.tapad.com
:scheme: https
:path: /tapestry/1?ta_partner_id=2052&ta_partner_did=k-TWbpu-_mzO5pZk6QJw2xO3-6hBnps98koqmNcA&ta_format=png
sec-ch-ua-platform: "Windows"
```

168. When called onto the site by Criteo, Tapad provides the Tapad ID and information from its ID Graph to Criteo so that Criteo can identify the individual visiting the website and target that person with hyper-specific advertising related to the individual's web activity pulled from any information that Defendants may possess about the user in that user's profile, which has now been connected to the Criteo Pixel via the Tapad ID.

169. The Criteo Pixel, in addition to calling a Tapad Pixel onto the Loan Depot website, calls 29 other pixels onto the Loan Depot website. These pixels belong to advertisers that oversee all stages of the tracking and real-time-bidding advertising processes. In addition to assisting Criteo with collecting information about visitors to the Loan Depot website, Tapad provides identity resolution services to these other pixels as well.

170. When a user selects the type of loan they are applying for, that information is disclosed in the URL of the loan depot website.

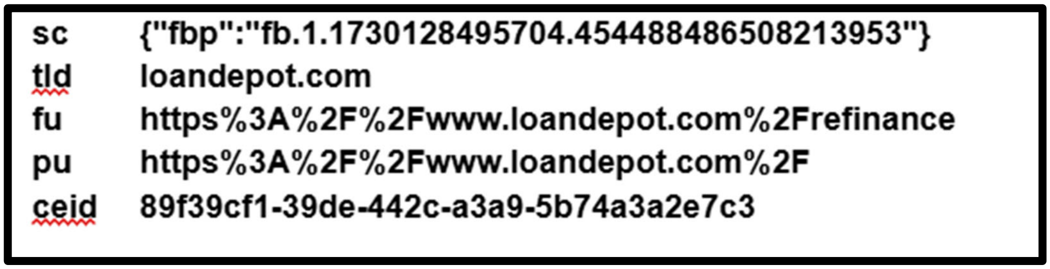


What does home mean to our customers?

Everything.

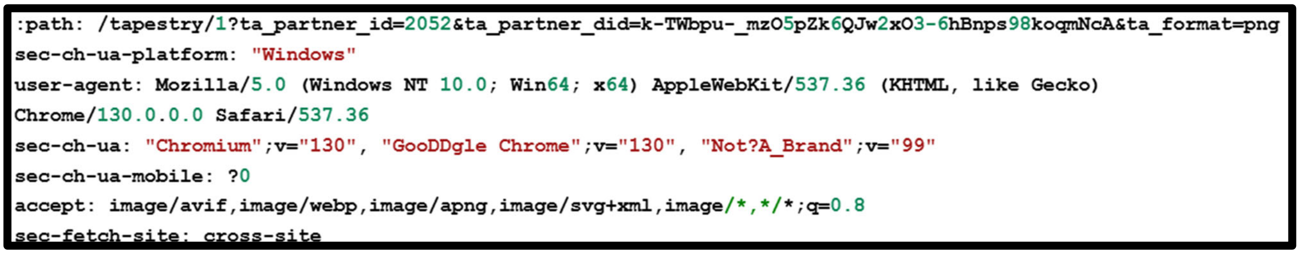
At loanDepot, we know home means everything to you, too. That's why we provide seamless mortgage solutions powered by technology and unrivaled customer service.

171. This full-string URL is collected by Criteo in real time as the user navigates through the application.



```
sc      {"fbp":"fb.1.1730128495704.454488486508213953"}
tld     loandepot.com
fu      https%3A%2F%2Fwww.loandepot.com%2Frefinance
pu      https%3A%2F%2Fwww.loandepot.com%2F
ceid    89f39cf1-39de-442c-a3a9-5b74a3a2e7c3
```

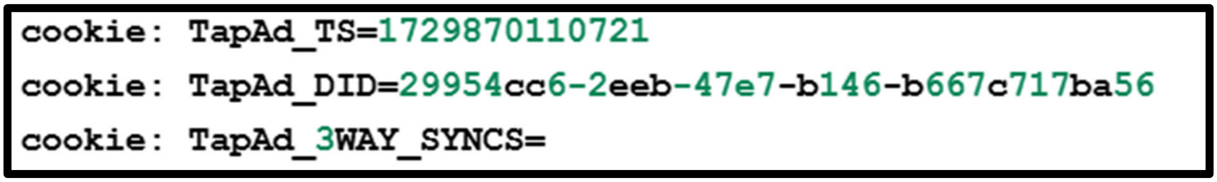
172. Tapad also collects a variety of identifiers and device information as described in detail above.



```
:path: /tapestry/1?ta_partner_id=2052&ta_partner_did=k-TWbpu-_mzO5pZk6QJw2xO3-6hBnps98koqmNcA&ta_format=png
sec-ch-ua-platform: "Windows"
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/130.0.0.0 Safari/537.36
sec-ch-ua: "Chromium";v="130", "GooDDgle Chrome";v="130", "Not?A_Brand";v="99"
sec-ch-ua-mobile: ?0
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
sec-fetch-site: cross-site
```

173. Tapad then adds this information to its profile on the individual. This profile is connected to the Tapad ID assigned to the individual and added to Defendants' ID Graph, Consumer View, and Consumer Sync described herein. This data added to an individual's profile increases its value to advertisers, who can serve ads related to finance to the individual.

174. In addition, when an internet user visits the Loan Depot website, Tapad loads its cookie onto the individual's browser as described above.



```
cookie: TapAd_TS=1729870110721
cookie: TapAd_DID=29954cc6-2eeb-47e7-b146-b667c717ba56
cookie: TapAd_3WAY_SYNCS=
```

175. Tapad then tracks the future web activity of the individual and adds that information to its consumer profile and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

### D. Zillow

176. Zillow's website, zillow.com, is an online resource for real estate renters and buyers nationwide. Website visitors can view listings for specific properties, search for properties in specific geographic areas, and apply to rent or buy specific properties.

177. What these users do not know is that five separate pixels, the Crowd Control Pixel, the Snap Pixel, the Pubmatic Pixel, the Rubicon Pixel and the Adsrvr Pixel are all loaded onto the Zillow website.[84]

//

//

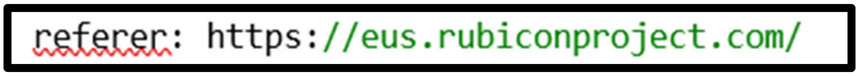
//

//

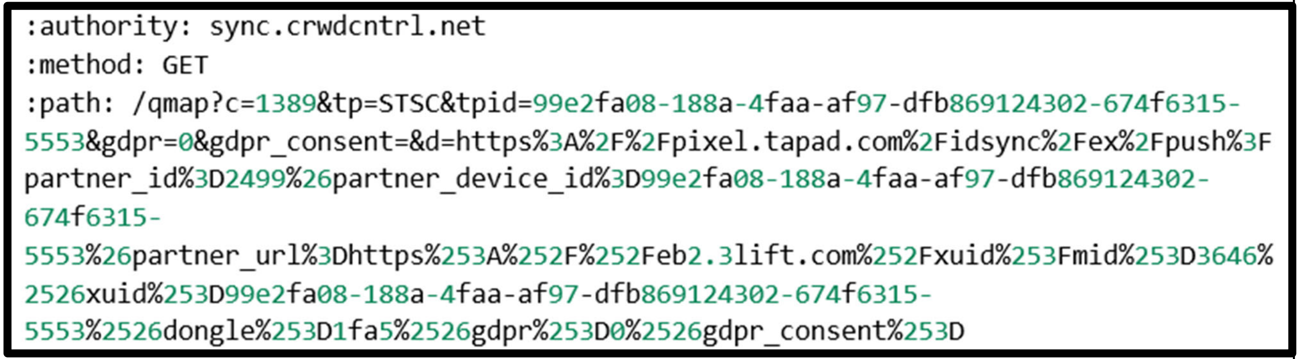
//

//

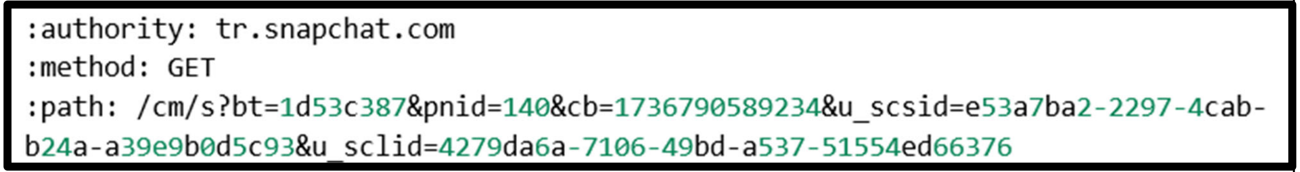
[84] The Crowd Control Pixel snippet was previously referenced in Factual Allegations § II.A.3, *supra*. Plaintiffs alleged this snippet was particularly privacy invasive because it involved combining the information held by three data brokers (Experian, Tapad, and Lotame) and using it to serve targeted advertisements to Zillow website users through the real-time bidding process, in conjunction with the TripleLift tracker.



```
referer: https://eus.rubiconproject.com/
```

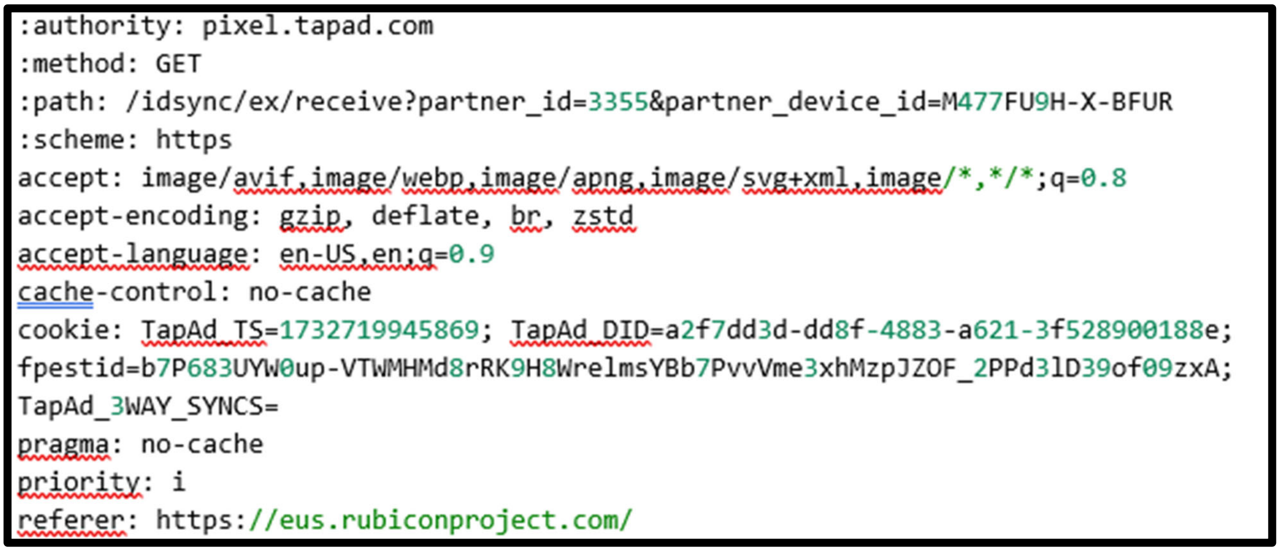


```
:authority: sync.crwdcntrl.net
:method: GET
:path: /qmap?c=1389&tp=STSC&tpid=99e2fa08-188a-4faa-af97-dfb869124302-674f6315-
5553&gdpr=0&gdpr_consent=&d=https%3A%2F%2Fpixel.tapad.com%2Fidsync%2Fex%2Fpush%3F
partner_id%3D2499%26partner_device_id%3D99e2fa08-188a-4faa-af97-dfb869124302-
674f6315-
5553%26partner_url%3Dhttps%253A%252F%252Feb2.3lift.com%252Fxuid%253Fmid%253D3646%
2526xuid%253D99e2fa08-188a-4faa-af97-dfb869124302-674f6315-
5553%2526dongle%253D1fa5%2526gdpr%253D0%2526gdpr_consent%253D
```



```
:authority: tr.snapchat.com
:method: GET
:path: /cm/s?bt=1d53c387&pnid=140&cb=1736790589234&u_scsid=e53a7ba2-2297-4cab-
b24a-a39e9b0d5c93&u_sclid=4279da6a-7106-49bd-a537-51554ed66376
```

178. Each pixel, independently, automatically calls a Tapad pixel onto the website when a user accesses the Zillow website.



```
:authority: pixel.tapad.com
:method: GET
:path: /idsync/ex/receive?partner_id=3355&partner_device_id=M477FU9H-X-BFUR
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cache-control: no-cache
cookie: TapAd_TS=1732719945869; TapAd_DID=a2f7dd3d-dd8f-4883-a621-3f528900188e;
fpestid=b7P683UYW0up-VTWMHMd8rRK9H8WrelmsYBb7PvvVme3xhMzpJZOF_2PPd3lD39of09zxA;
TapAd_3WAY_SYNCS=
pragma: no-cache
priority: i
referer: https://eus.rubiconproject.com/
```

179. As a user searches for and views properties on the Zillow website, the information is included in the URL for the Zillow website.

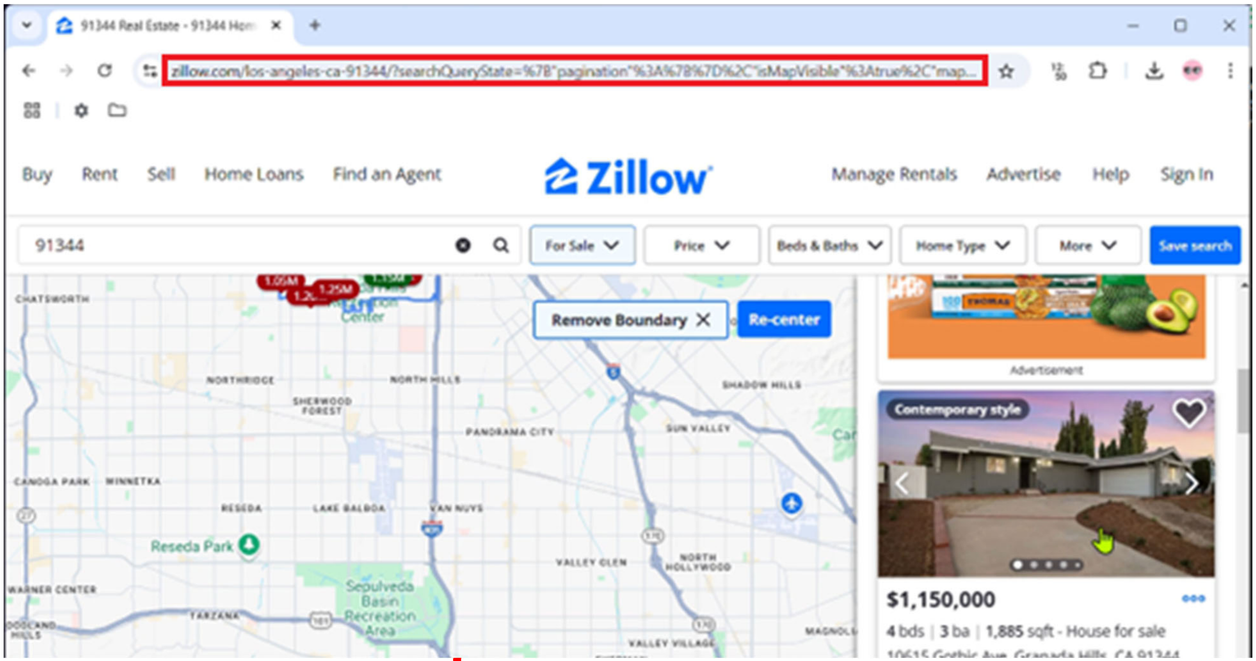
//

//

//

//

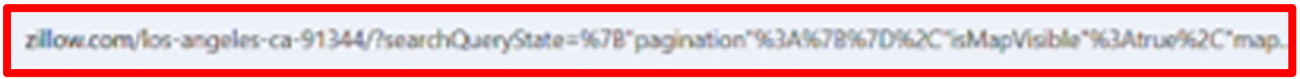
//

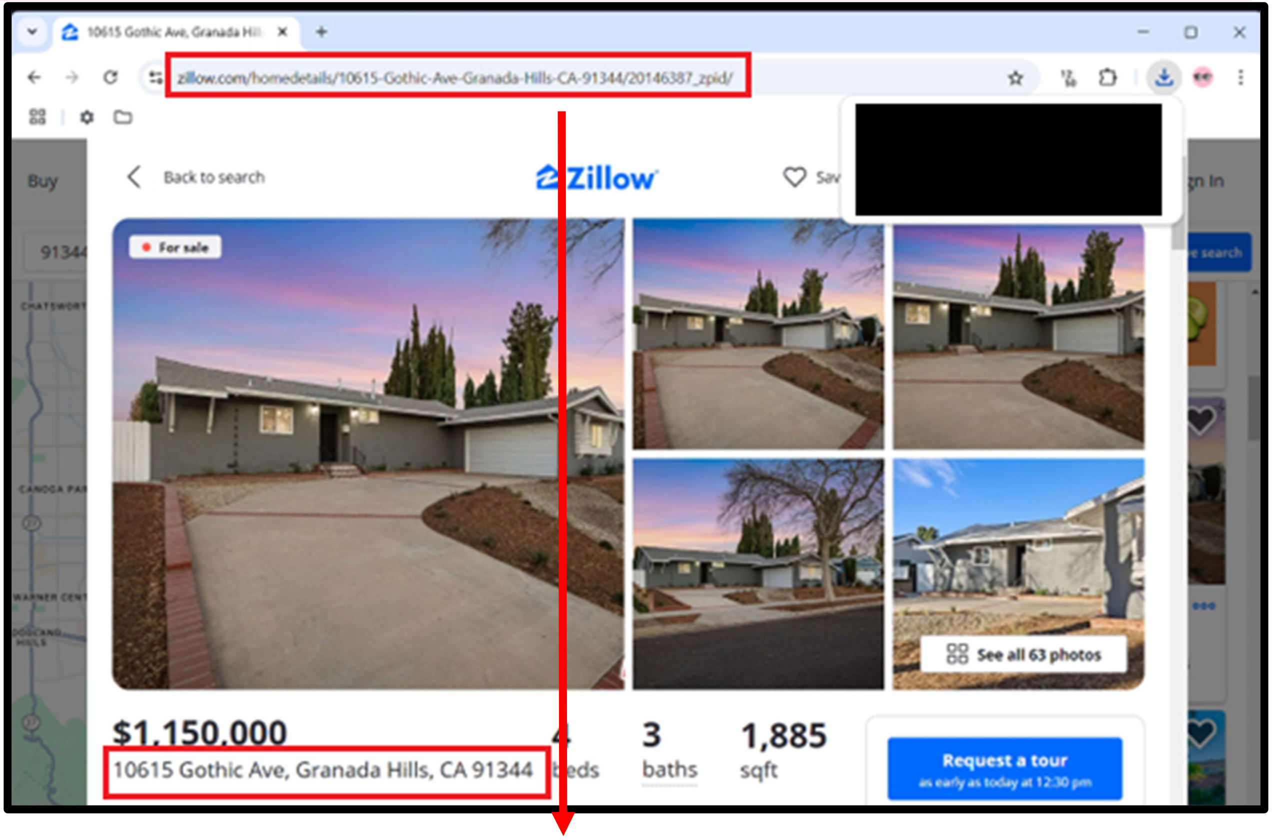


$1,150,000

4 bds | 3 ba | 1,885 sqft - House for sale

10615 Gothic Ave, Granada Hills, CA 91344


zillow.com/los-angeles-ca-91344/?searchQueryState=%7B"pagination"%3A%7B%7D%2C"isMapVisible"%3Atrue%2C"map...

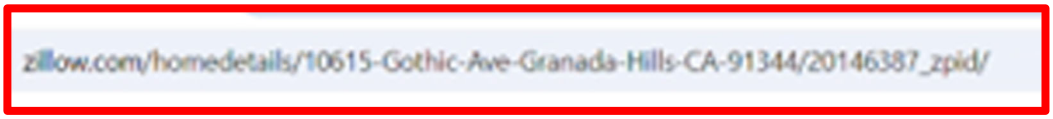

10615 Gothic Ave, Granada Hi
zillow.com/homedetails/10615-Gothic-Ave-Granada-Hills-CA-91344/20146387_zpid/
Back to search
Zillow
Sav
For sale
See all 63 photos
Request a tour
as early as today at 12:30 pm

[redacted]

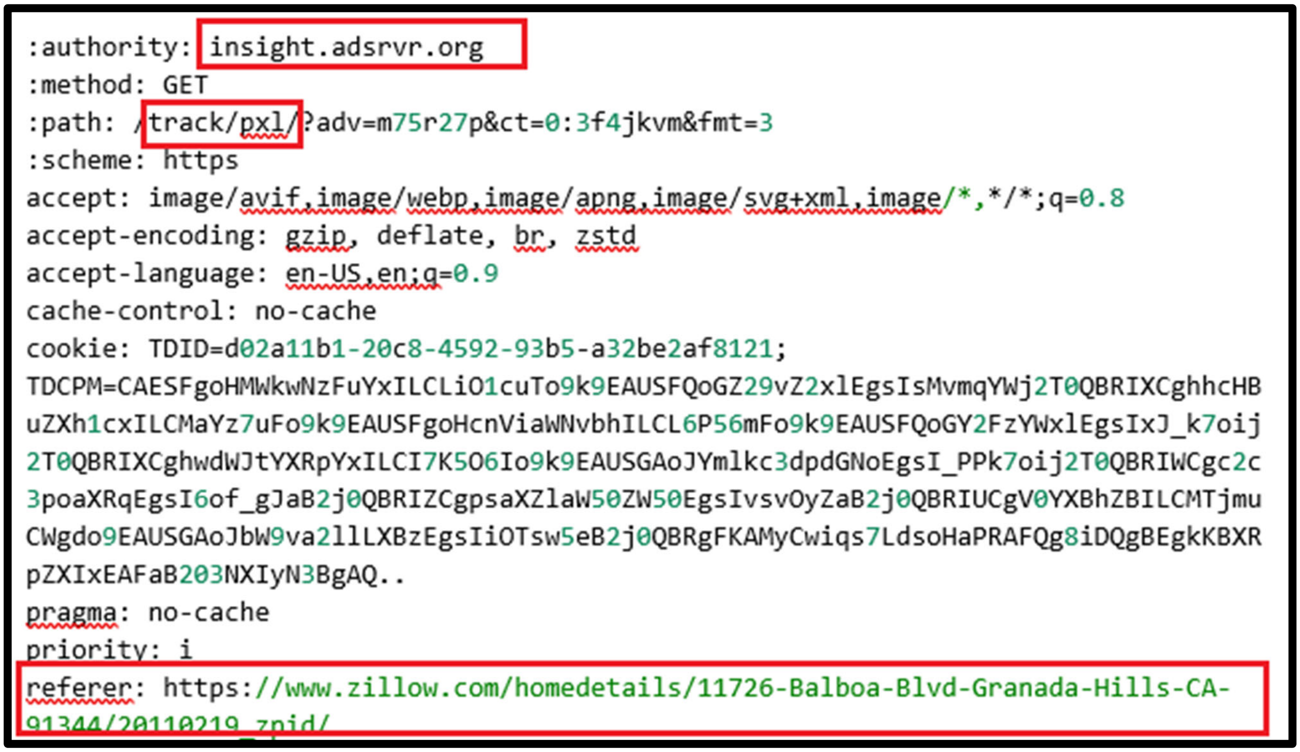
$1,150,000

10615 Gothic Ave, Granada Hills, CA 91344

4 beds 3 baths 1,885 sqft

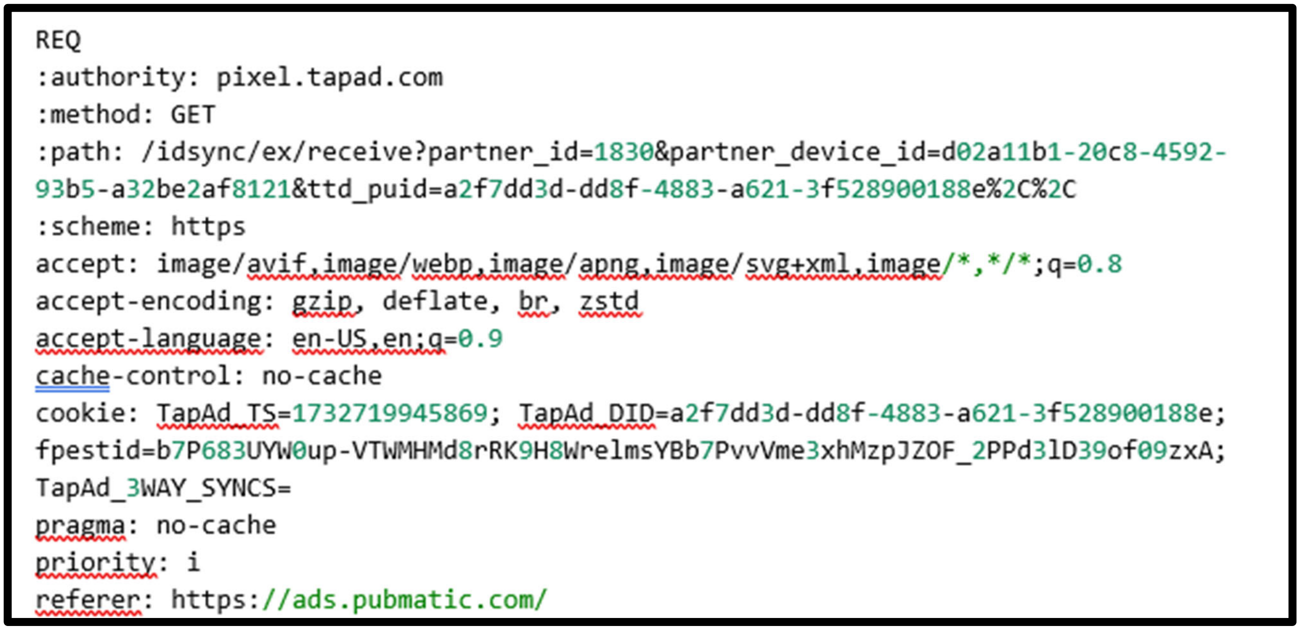

zillow.com/homedetails/10615-Gothic-Ave-Granada-Hills-CA-91344/20146387_zpid/

180. Each of the Partner Pixels intercepts the full-string URLs as the website visitor navigates the Zillow website, thus intercepting website visitors communications with the site about where they want to live and what types of properties they are interested in.



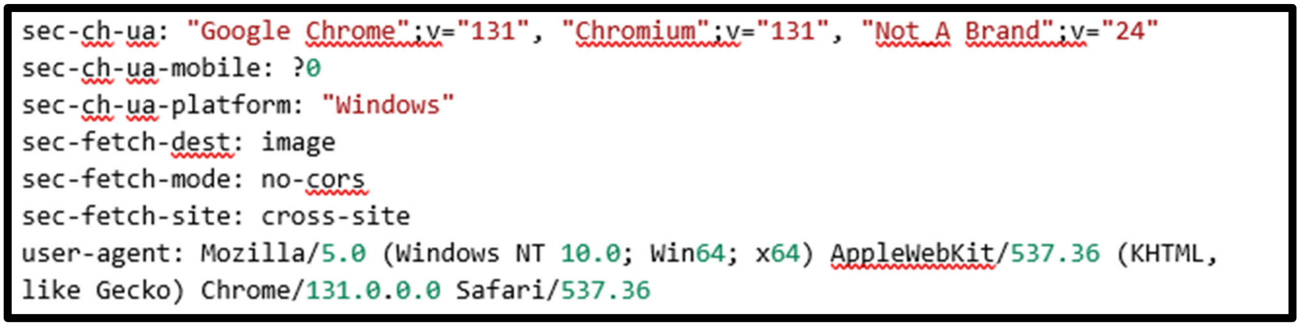
```
:authority: insight.adsrvr.org
:method: GET
:path: /track/pxl/?adv=m75r27p&ct=0:3f4jkvm&fmt=3
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cache-control: no-cache
cookie: TDID=d02a11b1-20c8-4592-93b5-a32be2af8121;
TDCPM=CAESFgoHMWkwNzFuYxILCLiO1cuTo9k9EAUSFQoGZ29vZ2xlEgsIsMvmqYWj2T0QBRIXCghhcHB
uZXh1cxILCMaYz7uFo9k9EAUSFgoHcnViaWNvbhILCL6P56mFo9k9EAUSFQoGY2FzYWxlEgsIxJ_k7oij
2T0QBRIXCghwdWJtYXRpYxILCI7K5O6Io9k9EAUSGAoJYmlkc3dpdGNoEgsI_PPk7oij2T0QBRIWCgc2c
3poaXRqEgsI6of_gJaB2j0QBRIZCgpsaXZlaW50ZW50EgsIvsvOyZaB2j0QBRIUCgV0YXBhZBILCMTjmu
CWgdo9EAUSGAoJbW9va2llLXBzEgsIiOTsw5eB2j0QBRgFKAMyCwiqs7LdsoHaPRAFQg8iDQgBEgkKBXR
pZXIxEAFaB203NXIyN3BgAQ..
pragma: no-cache
priority: i
referer: https://www.zillow.com/homedetails/11726-Balboa-Blvd-Granada-Hills-CA-
91344/20110219_zpid/
```

181. As described above, Tapad provides identity resolution services to each of the Partner Pixels loaded onto the Zillow website, allowing them to access the identity of the individual whose data they are collecting.



```
REQ
:authority: pixel.tapad.com
:method: GET
:path: /idsync/ex/receive?partner_id=1830&partner_device_id=d02a11b1-20c8-4592-
93b5-a32be2af8121&ttd_puid=a2f7dd3d-dd8f-4883-a621-3f528900188e%2C%2C
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cache-control: no-cache
cookie: TapAd_TS=1732719945869; TapAd_DID=a2f7dd3d-dd8f-4883-a621-3f528900188e;
fpestid=b7P683UYW0up-VTWMHMd8rRK9H8WrelmsYBb7PvvVme3xhMzpJZOF_2PPd3lD39of09zxA;
TapAd_3WAY_SYNCS=
pragma: no-cache
priority: i
referer: https://ads.pubmatic.com/
```

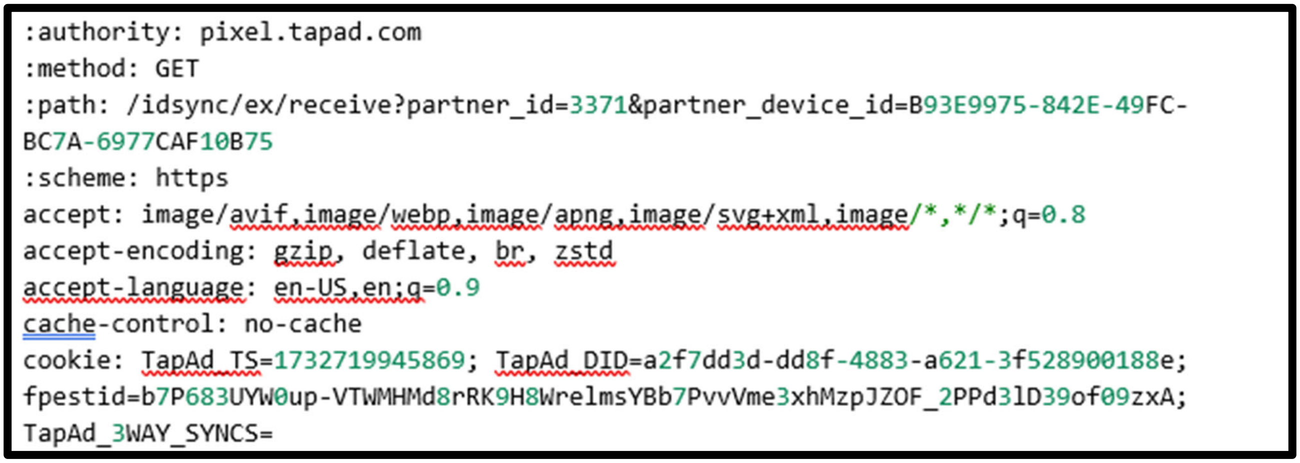
182. Tapad also collects a variety of identifiers and device information in the manner described in detail above.



```
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-dest: image
sec-fetch-mode: no-cors
sec-fetch-site: cross-site
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/131.0.0.0 Safari/537.36
```

183. Tapad then adds this information to its profile on the individual. This profile is connected to the Tapad ID assigned to the individual and added to Defendants' ID Graph, Consumer View, and Consumer Sync described herein. This data is added to an individual's profile and increases its value to advertisers, who can serve ads related to home loans, apartments for rent, and mortgages to the individual. Advertisers can also serve advertisements based on any other information that Defendants may possess about the user in that user's profile, which has now been connected to the Partner Pixels on the Zillow website via the Tapad ID.

184. In addition, when an internet user visits the Zillow website, Tapad loads its cookies onto the individual's browser as described above.



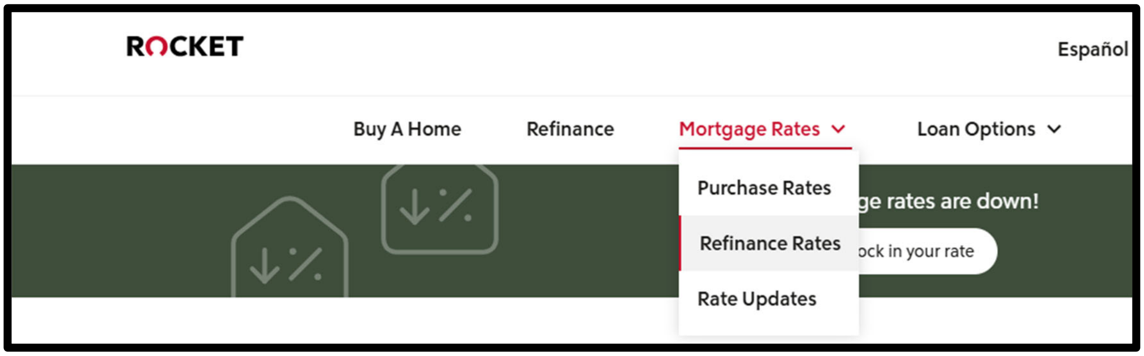
```
:authority: pixel.tapad.com
:method: GET
:path: /idsync/ex/receive?partner_id=3371&partner_device_id=B93E9975-842E-49FC-
BC7A-6977CAF10B75
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cache-control: no-cache
cookie: TapAd_TS=1732719945869; TapAd_DID=a2f7dd3d-dd8f-4883-a621-3f528900188e;
fpestid=b7P683UYW0up-VTWMHMd8rRK9H8WrelmsYBb7PvvVme3xhMzpJZOF_2PPd31D39of09zxA;
TapAd_3WAY_SYNCS=
```

185. Tapad then tracks the future web activity of the individual and adds that information to its consumer profile and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

## E. Rocket Mortgage

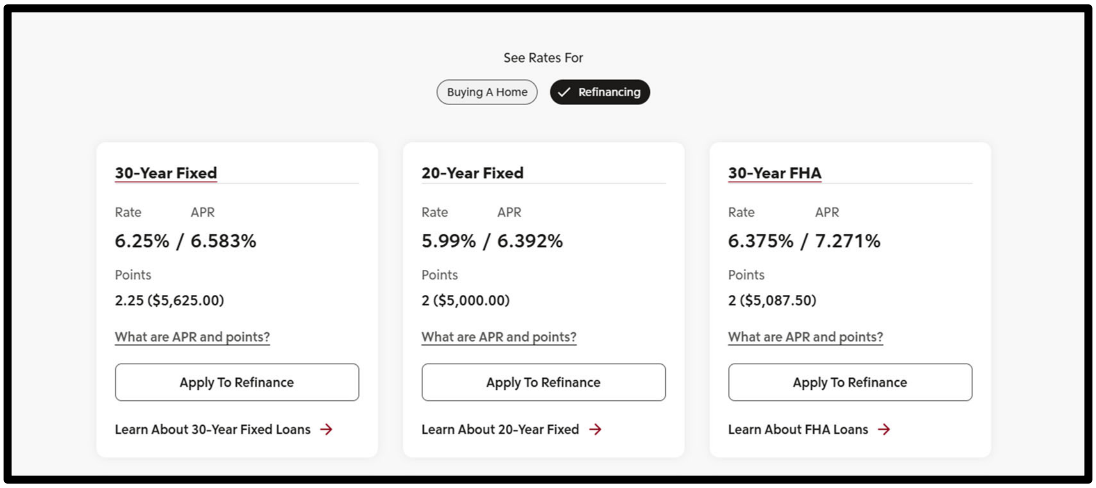
186. Rocket Mortgage is a company that operates rocketmortgage.com, a website where consumers can apply for and obtain home loans.

187. Consumers start by clicking a button for their desired action on the website:



188. As described above, when a button is clicked, in this case "refinance rates," that information is included in the detailed, descriptive URL of the website: https://www.rocketmortgage.com/refinance-rates.

189. After selecting the action, the user is prompted to select which refinancing option they wish to apply to:

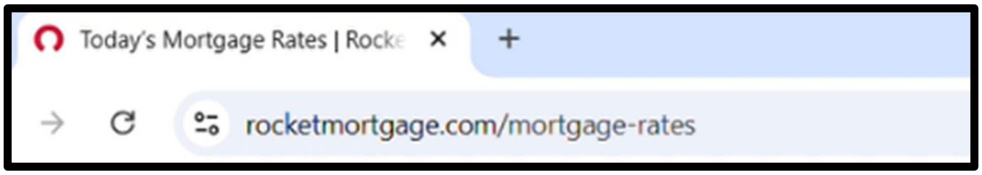


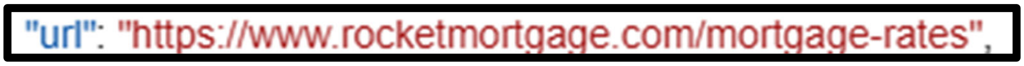
| 30-Year Fixed | 20-Year Fixed | 30-Year FHA |
|---|---|---|
| Rate / APR: 6.25% / 6.583% | Rate / APR: 5.99% / 6.392% | Rate / APR: 6.375% / 7.271% |
| Points: 2.25 ($5,625.00) | Points: 2 ($5,000.00) | Points: 2 ($5,087.50) |

190. The consumer then goes through the application, entering information and selecting buttons to answer questions related to the loan they are applying for. If approved, the consumer can "purchase" the loan on the Rocket Mortgage website.

191. Unbeknownst to consumers, the Snap Pixel is loaded onto all pages of rockermotgage.com. The Snap Pixel collects the URL of each page of the application and each

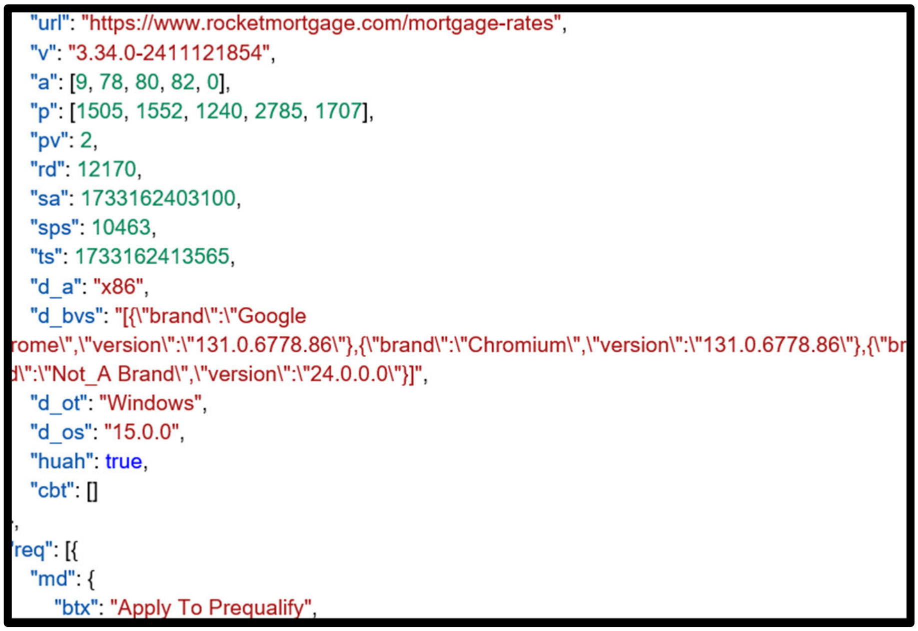
button clicked by the person applying for the loan, which allows Snapchat to capture information about which type of loan the person is requesting and their activity on the site.


Today's Mortgage Rates | Rocke
rocketmortgage.com/mortgage-rates

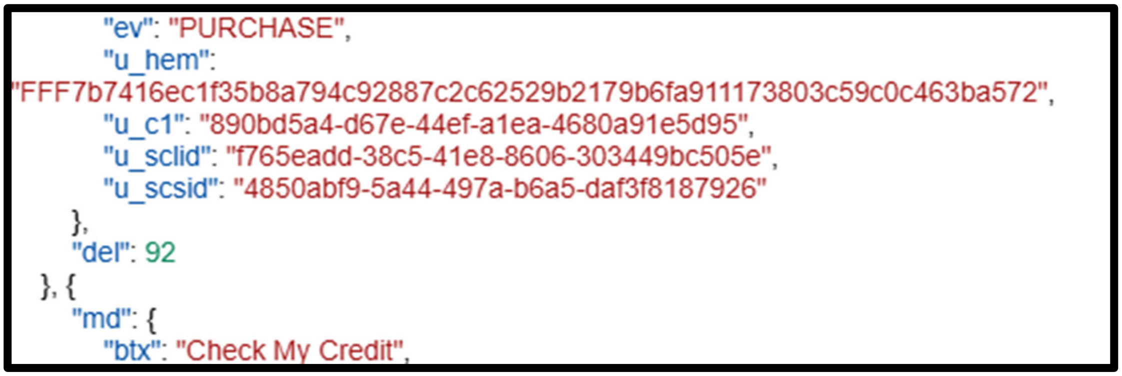


```
"url": "https://www.rocketmortgage.com/mortgage-rates",
```

192. The Snap pixel also collects button clicks (show next to the "btx" value below) which further allows it to collect the contents of communications with the Rocket Mortgage website.

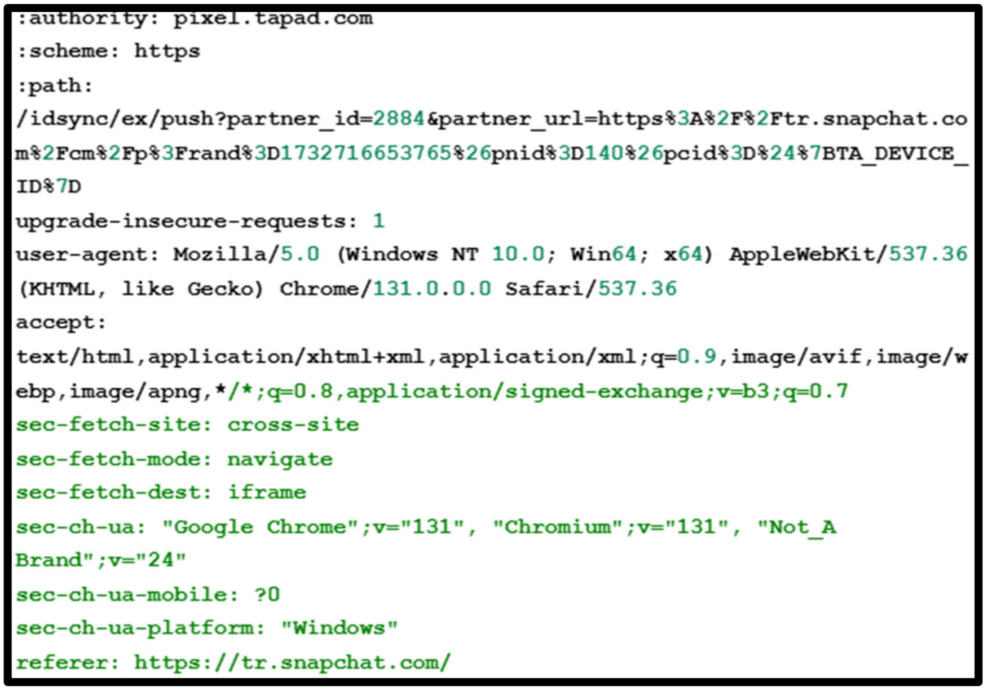


```
  "url": "https://www.rocketmortgage.com/mortgage-rates",
  "v": "3.34.0-2411121854",
  "a": [9, 78, 80, 82, 0],
  "p": [1505, 1552, 1240, 2785, 1707],
  "pv": 2,
  "rd": 12170,
  "sa": 1733162403100,
  "sps": 10463,
  "ts": 1733162413565,
  "d_a": "x86",
  "d_bvs": "[{\"brand\":\"Google
rome\",\"version\":\"131.0.6778.86\"},{\"brand\":\"Chromium\",\"version\":\"131.0.6778.86\"},{\"br
d\":\"Not_A Brand\",\"version\":\"24.0.0.0\"}]",
  "d_ot": "Windows",
  "d_os": "15.0.0",
  "huah": true,
  "cbt": []
,
req": [{
  "md": {
    "btx": "Apply To Prequalify",
```



```
        "ev": "PURCHASE",
        "u_hem":
"FFF7b7416ec1f35b8a794c92887c2c62529b2179b6fa911173803c59c0c463ba572",
        "u_c1": "890bd5a4-d67e-44ef-a1ea-4680a91e5d95",
        "u_sclid": "f765eadd-38c5-41e8-8606-303449bc505e",
        "u_scsid": "4850abf9-5a44-497a-b6a5-daf3f8187926"
      },
      "del": 92
    }, {
      "md": {
        "btx": "Check My Credit",
```

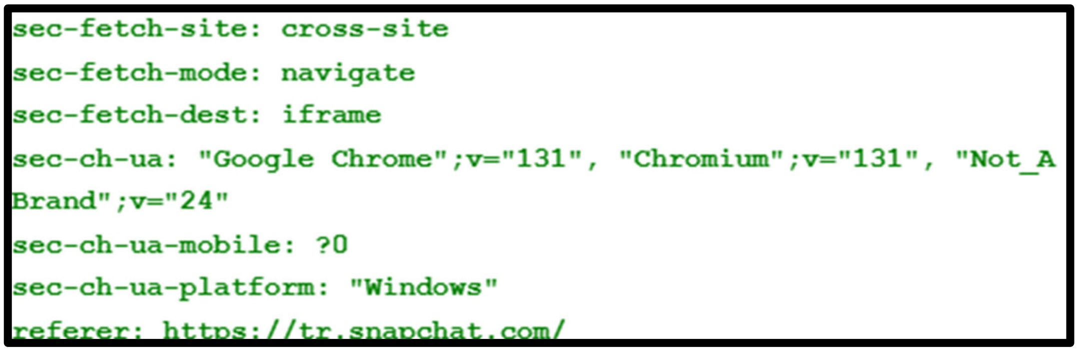
193. When an internet user visits the Rocket Mortgage website, the Snap Pixel automatically calls a Tapad pixel onto the website.



```
:authority: pixel.tapad.com
:scheme: https
:path:
/idsync/ex/push?partner_id=2884&partner_url=https%3A%2F%2Ftr.snapchat.co
m%2Fcm%2Fp%3Frand%3D1732716653765%26pnid%3D140%26pcid%3D%24%7BTA_DEVICE_
ID%7D
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
sec-fetch-site: cross-site
sec-fetch-mode: navigate
sec-fetch-dest: iframe
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A
Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
referer: https://tr.snapchat.com/
```

194. When called on to the site by Snapchat, Tapad provides the Tapad ID and information from its ID Graph to Snapchat so that Snapchat can identify the individual visiting the website and target that person with hyper-specific advertising related to their loan application on the Rocket Mortgage website. SnapChat can also target the user with advertisements related to any other information that Defendants may possess about the user in that user's profile, which has now been connected to the Snap Pixel via the Tapad ID.

195. Tapad also collects a variety of identifiers and device information in the manner described in detail above and is explicitly gathering "cross-site" data.

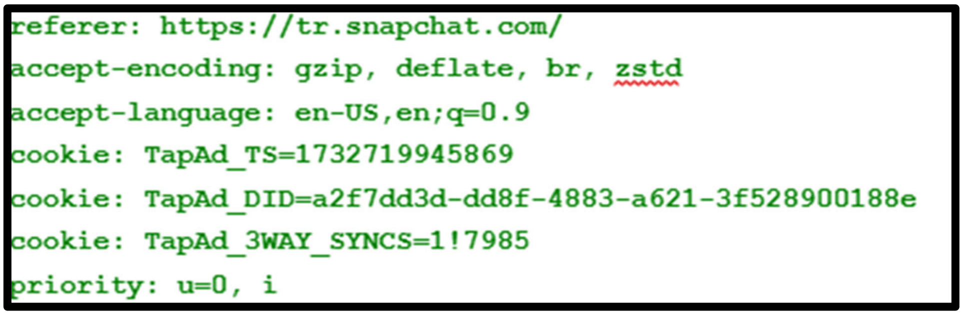


```
sec-fetch-site: cross-site
sec-fetch-mode: navigate
sec-fetch-dest: iframe
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A
Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
referer: https://tr.snapchat.com/
```

196. Tapad then adds this information to its profile on the individual. This profile is connected to the Tapad ID assigned to the individual and added to Defendants' ID Graph, Consumer

View, and Consumer Sync described herein. This data added to an individual's profile increases its value to advertisers, who can serve ads related to mental health treatment to the individual.

197. In addition, when an internet user visits the Rocket Mortgage website, Tapad loads its cookies onto the individual's browser as described above.



```
referer: https://tr.snapchat.com/
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cookie: TapAd_TS=1732719945869
cookie: TapAd_DID=a2f7dd3d-dd8f-4883-a621-3f528900188e
cookie: TapAd_3WAY_SYNCS=1!7985
priority: u=0, i
```

198. Tapad then tracks the future web activity of the individual and adds that information to its consumer profile and tracking products, as well as connecting that information to users being offered up for sale to advertisers as part of the real-time-bidding advertising process.

## IV. DEFENDANTS' SERVICES DEANONYMIZE USERS AND ENRICH DEFENDANTS, WEBSITE OPERATORS, AND PARTNER PIXELS ALIKE THROUGH REAL-TIME-BIDDING AND PROFILING INDIVIDUALS

### A. Defendants Combine The Data From All The Subject Websites With Other Data To Deanonymize Users

199. As a result of Tapad being called to thousands or millions of websites, Defendants are collecting various forms of PII and web activity records of nearly every American.

200. The information collected, on its own, is enough to identify the individual internet user. But this is only the first step in Defendant's practices of dragnet surveillance.

201. Defendants also combine the data from each and every website a person visits with other data collected by Experian to bolster the profiles of Experian sells as part of its products.

202. Experian specifically advertises that it can deanonymize the information it collects by "convert[ing] sensitive PII [personally identifiable information] data into actionable insights."[85]

[85] Justin Sherman, Duke Sanford Cyber Policy Program, Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy, at 1 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

203. This is consistent with Experian's business model, which "advertises data on 95% of the U.S. population, including information on 300 million consumers, 126 million living units, and 4.4 billion economic transactions spanning thousands of data attributes."[86]

204. This is further evidenced by the design of the Consumer View and Consumer Sync products, which by design combine the data collected on the internet with data from other sources, a process only possible if Experian knows the identity of the person being tracked.

205. In short, the detailed profiles on nearly every aspect of every American's life require Experian to match the identity of each individual with the data collected about them. This makes the profiles much more valuable to Experian's customers and increases Experian's profits by billions of dollars.

### B. The Partner Pixels Use The Profiles Created By Defendants To Enhance Their Advertising And Analytics Services

206. In addition to contributing vast amounts of data to Experian's data profiles, the data collected by Tapad is utilized by the partner pixels to conduct hyper-targeted advertising through the real-time-bidding process. *See* Factual Allegations § I.B, *supra*.

207. The Tapad identity resolution process is a key part of a complex ecosystem of pixels which deliver detailed user information to advertisers to increase the efficiency of those advertisements.

208. When Tapad shares website visitor information with a Pixel Partner, that partner (i) uses the information provided by Tapad to add information to its own data and advertising datasets and (ii) shares the identity information with other advertisers during the real-time-bidding delivery of advertisements.

209. For ads to be delivered as soon as a website user visits a site, multiple technology companies need access to detailed information about the identity and interests of the individual website visitor.

210. This information is provided by the Partner Pixels, who use Defendants' identity resolution services (which they pay for) to create and expand their own datasets, which they in turn

[86] *Id.*

disclose to other players in the real-time-bidding ecosystem as advertisements are delivered on websites.

211. Each time a user is selected by this network of advertisers to receive an ad, the advertisers "bid" on the user—meaning Defendants or the Partner Pixels are paid for the information they have stored about that user. Millions of these bids are made per day across the internet, demonstrating the immense value of the data Defendants improperly collect on Plaintiffs and Class Members.

212. As such, the improper collection of vast amounts of data on Plaintiffs and Class Members is done both for Defendants' profit and for the profit of the Partner Pixels.

## V. PLAINTIFFS' EXPERIENCES

### A. Plaintiff ZhiCheng Zhen

213. In or about February 2024, Plaintiff ZhiCheng Zhen visited the GEICO website while in California and took the necessary steps to receive an online quote for auto insurance.

214. Unbeknownst to Plaintiff Zhen, the Snap Pixel was loaded onto each page of the website.

215. When Plaintiff Zhen visited the GEICO website, the Snap Pixel called a Tapad pixel onto the website. The Tapad pixel installed three separate cookies onto Plaintiff Zhen's browser.

216. Both the Snap Pixel and the Tapad Pixel collected information about Plaintiff Zhen's device, browser, and tracked him as he navigated through the website.

217. Tapad provided Snap with identity resolution services so that Snap could deanonymize the data it collected on Plaintiff Zhen and sell it during the real-time-bidding process.

218. Tapad also collected information about Plaintiff Zhen, including the webpages he visited, his IP address, and fingerprint information about his device and browser, among others.

219. Defendants compiled this information into a profile on Plaintiff Zhen and added the bolstered profile to Experian's suite of data products described above.

220. Defendants also, by using the cookies loaded onto Plaintiff Zhen's browser, tracked his future web browsing activity across the internet and assisted other Partner Pixels in tracking him and wiretapping his communications with websites.

221. Plaintiff Zhen was unaware that Defendants were installing trackers on his browser, aiding in the wiretapping of his communications, deanonymizing his personal data, or collecting, selling, and disclosing his personal data, including data related to insurance, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor could Plaintiff Zhen have discovered these facts. Plaintiff Zhen did not become aware that he was being tracked on the GEICO website and across the internet by Defendants until October 2024.

222. Plaintiff Zhen did not provide his prior consent to Defendants to install trackers on his browser, aid in the wiretapping of his communications, deanonymize his personal data, or collect, sell, and disclose his personal data, including data related to insurance, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor did Defendants obtain a court order to do the same.

223. Plaintiff Zhen has, therefore, had his privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendants have been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Zhen.

### B. Plaintiff Marcus Johnson

224. In or about July 2022, Plaintiff Marcus Johnson visited the GEICO website while in California and took the necessary steps to receive an online quote for auto insurance.

225. Unbeknownst to Plaintiff Johnson, the Snap Pixel was loaded onto each page of the website.

226. When Plaintiff Johnson visited the GEICO website, the Snap Pixel called a Tapad pixel onto the website. The Tapad pixel installed three separate cookies onto his browser.

227. Both the Snap Pixel and the Tapad Pixel collected information about Plaintiff Johnson's device, browser, and tracked him as he navigated through the website.

228. Tapad provided Snap with identity resolution services so that Snap could deanonymize the data it collected on Plaintiff Johnson and sell it during the real-time-bidding process.

229. Tapad also collected information about Plaintiff Johnson, including the webpages he visited, his IP address, and fingerprint information about his device and browser, among others.

230. Defendants compiled this information into a profile on Plaintiff Johnson and added the bolstered profile to Experian's suite of data products described above.

231. Defendants also, by using the cookies loaded onto Plaintiff Johnson's browser, tracked his future web browsing activity across the internet and assisted other Partner Pixels in tracking him and wiretapping his communications with websites.

232. Plaintiff Johnson was unaware that Defendants were installing trackers on his browser, aiding in the wiretapping of his communications, deanonymizing his personal data, or collecting, selling, and disclosing his personal data, including data related to insurance, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor could Plaintiff Johnson have discovered these facts. Plaintiff Johnson did not become aware that he was being tracked on the GEICO website and across the internet by Defendants until November 2024.

233. Plaintiff Johnson did not provide his prior consent to Defendants to install trackers on his browser, aid in the wiretapping of his communications, deanonymize his personal data, or collect, sell, and disclose his personal data, including data related to insurance, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor did Defendants obtain a court order to do the same.

234. Plaintiff Johnson has, therefore, had his privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendants have been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Johnson.

### C. Plaintiff Jane Doe

235. In or about November 2024, Plaintiff Jane Doe visited the Mindbloom website while in California and purchased prescription ketamine therapy treatment.

236. Unbeknownst to Plaintiff Doe, the Magellan Pixel was loaded onto each page of the website.

237. When Plaintiff Doe visited the Mindbloom website, the Magellan Pixel called a Tapad pixel onto the website. The Tapad pixel installed three separate cookies onto her browser.

238. Both the Magellan Pixel and the Tapad Pixel collected information about Plaintiff Doe's device, browser, and tracked her as she navigated through the website.

239. The Magellan Pixel also received the URL of each page of the website Plaintiff Doe visited, allowing Magellan to know that Plaintiff Doe sought and purchased prescription ketamine therapy.

240. Tapad provided Magellan with identity resolution services so that Magellan could deanonymize the data it collected on Plaintiff Doe and sell it during the real-time-bidding process.

241. Tapad also collected information about Plaintiff Doe, including the webpages she visited, her IP address, and fingerprint information about her device and browser, among others.

242. Defendants compiled this information into a profile on Plaintiff Doe and added the bolstered profile to Experian's suite of data products described above.

243. Defendants also, by using the cookies loaded onto Plaintiff Doe's browser, tracked her future web browsing activity across the internet and assisted other Partner Pixels in tracking her and wiretapping her communications with websites.

244. Plaintiff Doe was unaware that Defendants were installing trackers her browser, aiding in the wiretapping of her communications, deanonymizing her personal data, or collecting, selling, and disclosing her personal data, including data about her medication and health status, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor could Plaintiff Doe have discovered these facts. Plaintiff Doe did not become aware that she was being tracked on the Mindbloom website and across the internet by Defendants until November 2024.

245. Plaintiff Doe did not provide her prior consent to Defendants to install trackers on her browser, aid in the wiretapping of her communications, deanonymize her personal data, or collect, sell, and disclose her personal data, including data about her medication and health status, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor did Defendants obtain a court order to do the same.

246. Plaintiff Doe has, therefore, had her privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendants have been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Doe.

247. Plaintiff Doe has, therefore, had her privacy invaded by Defendant's violations of CIPA §631(a) and § 638.51(a) and Defendants have been unjustly enriched by the sale of the improperly collected data concerning Plaintiff Doe.

### D. Plaintiff Kelda McKinney

248. In or about December 2020, Plaintiff Kelda McKinney visited the Loan Depot website while in California and applied for a mortgage.

249. Unbeknownst to Plaintiff McKinney, the Criteo Pixel was loaded onto each page of the website.

250. When Plaintiff McKinney visited the Loan Depot website, the Criteo Pixel called a Tapad pixel onto the website. The Tapad pixel installed three separate cookies onto her browser.

251. Both the Criteo Pixel and the Tapad Pixel collected information about Plaintiff McKinney's device, browser, and tracked her as she navigated through the website.

252. The Criteo Pixel, by receiving the full-string URL of each page of the website, intercepted Plaintiff McKinney's confidential communications with the Loan Depot website, including the type of loan she was seeking and the fact that she submitted an application.

253. These interceptions happened in real time as the information was entered into the Loan Depot website.

254. Tapad provided Criteo with identity resolution services so that Criteo could deanonymize the data it collected on Plaintiff McKinney and sell it during the real-time-bidding process.

255. Tapad and Criteo also shared the information they collected about Plaintiff McKinney with the 28 other Partner Pixels called onto the Loan Depot Website by the Criteo Pixel to facilitate the delivery of advertisements to Plaintiff McKinney.

256. Tapad also collected information about Plaintiff McKinney, including the webpages she visited, her IP address, and fingerprint information about her device and browser, among others.

257. Defendants compiled this information into a profile on Plaintiff McKinney and added the bolstered profile to Experian's suite of data products described above.

258. Defendants also, by using the cookies loaded onto Plaintiff McKinney's browser, tracked her future web browsing activity across the internet and assisted other Partner Pixels in tracking her and wiretapping her communications with websites.

259. Plaintiff McKinney was unaware that Defendants were installing trackers her browser, aiding in the wiretapping of her communications, deanonymizing her personal data, or collecting, selling, and disclosing her personal data, including data about her mortgage, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor could Plaintiff McKinney have discovered these facts. Plaintiff McKinney did not become aware that she was being tracked on the Loan Depot website and across the internet by Defendants until January 2025.

260. Plaintiff McKinney did not provide her prior consent to Defendants to install trackers on her browser, aid in the wiretapping of her communications, deanonymize her personal data, or collect, sell, and disclose her personal data, including data about her mortgage, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor did Defendants obtain a court order to do the same.

261. Plaintiff McKinney has, therefore, had her privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendants have been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff McKinney.

### E. Plaintiff Dilara Uskup

262. In or about December 2024, Plaintiff Dilara Uskup visited the Zillow website while in California and searched for properties for rent and purchase.

263. Unbeknownst to Plaintiff Uskup, the Crowd Control Pixel, the Snap Pixel, the Pubmatic Pixel, the Rubicon Pixel and the Adsrvr Pixel were each loaded onto each page of the website.

264. When Plaintiff Uskup visited the Zillow website, each Partner Pixel called a Tapad pixel onto the website. Each Tapad pixel installed three separate cookies onto her browser.

265. Each Partner Pixel and the Tapad Pixels collected information about Plaintiff Uskup's device, browser, and tracked her as she navigated through the website.

266. Each Partner Pixel, by receiving the full-string URL of each page of the website, intercepted Plaintiff Uskup's confidential communications with the Zillow website, including her geographic location and the specific properties that Plaintiff Uskup clicked on, viewed, and saved.

267. These interceptions happened in real time as the information was entered into the Zillow website.

268. Tapad provided each Partner Pixel with identity resolution services so that each Partner Pixel could deanonymize the data it collected on Plaintiff Uskup and sell it during the real-time-bidding process.

269. Tapad also collected information about Plaintiff Uskup, including the properties she viewed, her IP address, and fingerprint information about her device and browser, among others.

270. Defendants compiled this information into a profile on Plaintiff Uskup and added the bolstered profile to Experian's suite of data products described above.

271. Defendants also, by using the cookies loaded onto Plaintiff Uskup's browser, tracked her future web browsing activity across the internet and assisted other Partner Pixels in tracking her and wiretapping her communications with websites.

272. Plaintiff Uskup was unaware that Defendants were installing trackers her browser, aiding in the wiretapping of her communications, deanonymizing her personal data, or collecting, selling, and disclosing her personal data, including data about her living situation, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor could Plaintiff Uskup have discovered these facts. Plaintiff Uskup did not become aware that she was being tracked on the Zillow website and across the internet by Defendants until January 2025.

273. Plaintiff Uskup did not provide her prior consent to Defendants to install trackers on her browser, aid in the wiretapping of her communications, deanonymize her personal data, or collect, sell, and disclose her personal data, including data about her living situation, to advertising

technology companies, other data brokers, or any person or entity doing business with Defendants. Nor did Defendants obtain a court order to do the same.

274. Plaintiff Uskup has, therefore, had her privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendants have been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Uskup.

### F. Plaintiff Marc Russo

275. In or about December 2023, Plaintiff Marc Russo visited the Rocket Mortgage website while in California and applied for a mortgage.

276. Unbeknownst to Plaintiff Russo, the Snap Pixel was loaded onto each page of the website.

277. When Plaintiff Russo visited the Rocket Mortgage website, the Snap Pixel called a Tapad pixel onto the website. The Tapad pixel installed three separate cookies onto his browser.

278. Both the Snap Pixel and the Tapad Pixel collected information about Plaintiff Russo's device, browser, and tracked him as he navigated through the website.

279. The Snap Pixel, both by receiving the detailed descriptive URL of each page of the website and by intercepting button click event data as described above, intercepted Plaintiff Russo's confidential communications with the Rocket Mortgage website, including the type of loan he was seeking and when he planned to purchase property.

280. These interceptions happened in real time as the information was entered into the Rocket Mortgage website.

281. Tapad provided Snapchat with identity resolution services so that Snapchat could deanonymize the data it collected on Plaintiff Russo and sell it during the real-time-bidding process.

282. Tapad also collected information about Plaintiff Russo, including the webpages he visited, his IP address, and fingerprint information about his device and browser, among others.

283. Defendants compiled this information into a profile on Plaintiff Russo and added the bolstered profile to Experian's suite of data products described above.

284. Defendants also, by using the cookies loaded onto Plaintiff Russo's browser, tracked his future web browsing activity across the internet and assisted other Partner Pixels in tracking him and wiretapping his communications with websites.

285. Plaintiff Russo was unaware that Defendants were installing trackers his browser, aiding in the wiretapping of his communications, deanonymizing his personal data, or collecting, selling, and disclosing his personal data, including information about his mortgage, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor could Plaintiff Russo have discovered these facts. Plaintiff Russo did not become aware that he was being tracked on the Rocket Mortgage website and across the internet by Defendants until November 2024.

286. Plaintiff Russo did not provide his prior consent to Defendants to install trackers on his browser, aid in the wiretapping of her communications, deanonymize his personal data, or collect, sell, and disclose his personal data, including information about his mortgage, to advertising technology companies, other data brokers, or any person or entity doing business with Defendants. Nor did Defendants obtain a court order to do the same.

287. Plaintiff Russo has, therefore, had his privacy invaded by Defendant's violations of CIPA §§ 631(a) and 638.51(a), and Defendants have been unjustly enriched by the disclosure and sale of the improperly collected data concerning Plaintiff Russo.

## CLASS ALLEGATIONS

288. **Class Definition:** Plaintiffs seek to represent a class of similarly situated individuals defined as follows:

> All persons in the United States whose personal information, communications, or private information, or data derived from their personal information, communications, or private information, was used to create a profile and made available for sale or use through Defendants' ID Graph, Consumer View, Consumer Sync, or otherwise.

289. **California Subclass**: Plaintiffs also seek to represent a subclass of similarly situated individuals defined as follows:

> All California citizens in the United States whose personal information, communications, or private information, or data

> derived from their personal information, communications, or private information, was used to create a profile and made available for sale or use through Defendants' ID Graph, Consumer View, Consumer Sync, or otherwise.

290. The Class and California Subclass shall be collectively referred to as the "Classes," and Members of the Class and Subclass will collectively be referred to as "Class Members," unless it is necessary to differentiate them.

291. Excluded from the Classes are Defendants, any affiliate, parent, or subsidiary of any Defendant; any entity in which any Defendant has a controlling interest; any officer director, or employee of any Defendant; any successor or assign of any Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

292. **<u>Numerosity</u>**. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiffs at this time; however, it is estimated that there are tens or hundreds of millions of individuals in the Classes. The identity of such membership is readily ascertainable from Defendants' records and non-party records, such as those of Defendants' customers and advertising partners.

293. **<u>Typicality</u>**. Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs, like all Class Members, had their information collected and made available for sale by Defendants through the use of comprehensive user profiles compiled about Plaintiffs.

294. **<u>Adequacy</u>**. Plaintiffs are fully prepared to take all necessary steps to represent fairly and adequately the interests of the Classes. Plaintiffs' interests are coincident with, and not antagonistic to, those of the members of the Classes. Plaintiffs are represented by attorneys with experience in the prosecution of class action litigation generally and in the field of digital privacy litigation specifically. Plaintiffs' attorneys are committed to vigorously prosecuting this action on behalf of the members of the Classes.

295. **<u>Commonality/Predominance</u>**. Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members because

Defendants have acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendants' wrongful conduct. Questions of law and fact common to the Classes include:

(a) Whether Defendants' acts and practices alleged herein constitute egregious breaches of social norms;

(b) Whether Defendants acted intentionally in violating Plaintiffs' and Class Members' privacy rights under the California Constitution or common law;

(c) Whether Defendants were unjustly enriched as a result of their violations of Plaintiffs' and Class Members' privacy rights; and

(d) Whether Plaintiffs and Class Members are entitled to damages under CIPA or any other relevant statute;

296. **Superiority**: Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiffs know of no special difficulty to that would be encountered by litigating this action that would preclude its maintenance as a class action.

## CAUSES OF ACTION

### COUNT I
### Intrusion Upon Seclusion

297. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

298. Plaintiffs bring this claim individually and on behalf of the Classes against Defendants.

299. Plaintiffs bring this claim pursuant to California law.

300. To state a claim for intrusion upon seclusion "[Plaintiffs] must possess a legally

protected privacy interest … [Plaintiffs'] expectations of privacy must be reasonable … [and Plaintiffs] must show that the intrusion is so serious in 'nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.'" *Hernandez v. Hillsides, Inc*. 47 Cal. 4th 272, 286-87 (2009).

301. Plaintiffs and Class Members have an interest in: (i) precluding the dissemination and/or misuse of their sensitive, confidential communications and information; and (ii) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to highly intrusive surveillance at every turn.

302. By conducting such widespread surveillance, Defendants intentionally invaded Plaintiffs' and Class Members' privacy rights, as well as intruded upon Plaintiffs' and Class Members' seclusion.

303. Plaintiffs and Class Members had a reasonable expectation that their communications, identities, personal activities, health and other data would remain confidential.

304. Plaintiffs and Class Members did not and could not authorize Defendants to intercept data on every aspect of their lives and activities.

305. The conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

(a) Defendants engage in widespread data collection and interception of Plaintiffs' and Class Members' internet and app activity, including their communications with websites and apps, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.

(b) Defendants combine the information collected on websites and apps with offline information also gathered on individuals to create the Consumer View and Consumer Sync products.

(c) Defendants create comprehensive profiles based on this online and offline data, which violates Plaintiffs' Class Members' common law right to privacy and the control of their personal information.

(d) Defendants sell or disclose these profiles, which contain the data improperly collected about Plaintiffs and Class

> Members, to an unknown number of advertisers for use in the real-time-bidding process, which likewise violates Plaintiffs' Class Members' common law right to privacy and the control of their personal information.

306. Defendants' amassment of electronic information reflecting all aspects of Plaintiffs' and Class Members' lives into profiles for future or present use is in and of itself a violation of their right to privacy in light of the serious risk these profiles pose to their autonomy.

307. In addition, those profiles are and can be used to further invade Plaintiffs' and Class Members' privacy by, for example. allowing third parties to learn intimate details of their lives and target them for advertising, political, and other purposes, as described herein, thereby harming them by selling this data to advertisers and other data brokers without their consent.

308. Accordingly, Plaintiff and Class and California Subclass Members seek all relief available for invasion of privacy claims under common law.

## <u>COUNT II</u>
## Violation Of The California Invasion of Privacy Act
## Cal. Penal Code § 631(a)

309. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

310. Plaintiffs bring this claim individually and on behalf of the California Subclass against Defendants.

311. The California Legislature enacted the CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

312. The California Supreme Court has repeatedly stated the "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas*, 38 Cal. 3d at 363 (emphasis added, internal quotations omitted). This restriction is based on the "substantial distinction … between the secondhand repetition of the contents of a conversation and *its*

*simultaneous dissemination to an unannounced second auditor*, whether that auditor be a person or mechanical device." *Id.* at 361 (emphasis added). Such "simultaneous dissemination" "denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements." *Id.*; *see also Reporters Committee for Freedom of Press*, 489 U.S. at 763 ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

313. Further, "[t]hough written in terms of wiretapping, Section 631(a) applies to Internet communications." *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022). Indeed, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013). This accords with the fact that "the California Supreme Court has [] emphasized that all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purposes of CIPA." *Javier*, 2022 WL 1744107, at *2. "Thus, when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

314. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

315. To avoid liability under CIPA § 631(a), a defendant must show it had the consent of *all* parties to a communication, and that such consent was procured *prior to* the interception occurring. *See Javier*, 2022 WL 1744107, at *2.

316. Defendants' various Tapad pixels and SDKs are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

317. Defendants are each "separate legal entit[ies] that offer[] [a] 'software-as-a-service' and not merely [] passive device[s]." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, Defendants have the capability to use the wiretapped information for a purpose other than simply recording the communications and providing the communications to website operators. Accordingly, Defendants were each third parties to any communication between Plaintiffs and California Subclass Members, on the one hand, and any of the websites at issue, on the other. *Id*. at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

318. At all relevant times, Defendants willfully and without the consent of all parties to the communication, and in an unauthorized manner, read, attempted to read, and learned the contents the electronic communications of Plaintiffs and California Subclass Members, on the one hand, and the websites at issue, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

319. At all relevant times, Defendants uses those intercepted communications, including but not limited to building comprehensive user profiles that are offered for disclosure or sale in real-time bidding to prospective advertisers.

320. Plaintiffs and California Subclass Members did not provide their prior consent to Defendants' intentional interception, reading, learning, recording, collection, and usage of Plaintiffs'

and California Subclass Members' electronic communications.

321. The wiretapping of Plaintiffs and California Subclass Members occurred in California, where Plaintiffs and California Subclass Members accessed the websites, where Defendants' Tapad pixels were loaded on Plaintiffs' and California Subclass Members' browsers, and where Defendants routed Plaintiffs' and California Subclass Members' electronic communications to Defendants' servers.

322. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and California Subclass Members have been injured by Defendants' violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

## <u>**COUNT III**</u>
### **Violation Of The California Invasion Of Privacy Act,**
### **Cal. Penal Code § 638.51(a)**

323. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

324. Plaintiffs bring this claim individually and on behalf of the proposed California Subclass against Defendants.

325. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

326. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

327. A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

328. In plain English, a "pen register" is a "device or process" that records *outgoing* information, while a "trap and trace device" is a "device or process" that records *incoming* information.

329. For example, if a user sends an email, a "pen register" might record the email address it was sent from, the email address the email was sent to, and the subject line—because this is the user's *outgoing* information. On the other hand, if that same user receives an email, a "trap and trace device" might record the email address it was sent from, the email address it was sent to, and the subject line—because this is *incoming* information that is being sent to that same user.

330. Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology has advanced, however, courts have expanded the application of these surveillance devices. This, combined with the California Supreme Court's mandate to read provisions of the CIPA broadly to protect privacy rights, has led courts to apply CIPA § 638.50 to internet tracking technologies similar to the Defendants' technologies at issue here. *See*, *e.g.*, *Shah v. Fandom, Inc.*, --- F. Supp. 3d ---, 2024 WL 4539577, at *21 (N.D. Cal. Oct. 21, 2024) (finding trackers were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educ. Sys. Inc.*, --- F. Supp. 3d ---, 2024 WL 3561367, at *3 (C.D. Cal. July 25, 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and 638.51."); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (referencing CIPA's "expansive language" when finding software provided by data broker was a "pen register").

331. The Tapad pixels and the cookies Tapad installed on Plaintiffs' and California Subclass Members' browsers, to the extent they do not intercept "contents" of communications as defined in CIPA § 631(a), are "pen registers" because they are "device[s] or process[es]" that "capture" the "routing, addressing, or signaling information"—the IP address, geolocation, device information, and other persistent identifiers—from the electronic communications transmitted by Plaintiffs' and California Subclass Members' computers or smartphones. Cal. Penal Code § 638.50(b); *see also Shah,* 2024 WL 4539577, at *3; *Mirmalek*, 2024 WL 4102709, at *3.

332. At all relevant times, Defendants installed the Tapad pixels and cookies—which are pen registers—on Plaintiff's and California Subclass Members' browsers, which enabled Defendants to collect Plaintiff's and California Subclass Members' IP addresses, geolocation, device information, and other persistent identifiers from the websites they visited. Defendants then used the Tapad pixels and cookies to build comprehensive user profiles, which were used to unjustly enrich Defendants and its clients by linking and enhancing Plaintiff's and California Subclass Members' data when it is provided to advertisers through the real-time bidding process.

333. Plaintiffs and California Subclass Members did not provide their prior consent to Defendants' installation or use of the Tapad pixels, cookies, and other tracking technology at issue.

334. Defendants did not obtain a court order to install or use the Tapad pixels, cookies, and other tracking technology at issue.

335. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and California Subclass Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

## <u>COUNT IV</u>
## Unjust Enrichment

336. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

337. Plaintiffs bring this claim individually and on behalf of the Class against Defendants Experian Data Corporation and Experian Information Solutions, Inc., and on behalf of the California Subclass against Defendants Experian PLC and Tapad, Inc.

338. In both cases, Plaintiffs bring this claim pursuant to California law.

339. Defendants have wrongfully and unlawfully trafficked in the named Plaintiffs' and Class Members' personal information and other personal data without their consent for substantial profits.

340. Plaintiffs' and Class Members' personal information and data have conferred an economic benefit on Defendants, which was collected and used by Defendants without consent.

341. Defendants have been unjustly enriched at the expense of Plaintiffs and Class Members, and have unjustly retained the benefits of their unlawful and wrongful conduct.

342. It would be inequitable and unjust for Defendants to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

343. Plaintiffs and Class Members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Defendants obtained as a result of their unlawful and wrongful conduct.

344. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant.

345. Defendants have been unjustly enriched by virtue of their violations of Plaintiffs' and California Class members' legally protected rights to privacy as alleged herein, entitling Plaintiffs and California Class members to restitution of Defendants' enrichment. "[T]he consecrated formula 'at the expense of another' can also mean 'in violation of the other's legally protected rights,' without the need to show that the claimant has suffered a loss." RESTATEMENT (THIRD) OF RESTITUTION § 1, cmt. a.

346. Defendants were aware of the benefit conferred by Plaintiffs. Indeed, Defendants' data-brokerage products are premised entirely on the sale of such data to third parties. Defendants therefore acted in conscious disregard of the rights of Plaintiffs and Class and California Subclass Members and should be required to disgorge all profit obtained therefrom to deter Defendants and others from committing the same unlawful actions again.

## **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, seek judgment against Defendant, as follows:

(a) For an order certifying the Classes pursuant to Fed. R. Civ. P. 23, naming Plaintiffs as the representatives of the Classes, and naming Plaintiffs' attorneys as Class Counsel to represent the Classes.

(b) For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;

(c) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;

(d) For pre- and post-judgment interest on all amounts awarded; and

(e) For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit.

## **JURY TRIAL DEMANDED**

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a trial by jury of all issues so triable.

Dated: January 29, 2025

Respectfully submitted,

**BURSOR & FISHER, P.A.**

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta (State Bar No. 354768)
Max S. Roberts (*Pro Hac Vice Forthcoming*)
Victoria X. Zhou (*Pro Hac Vice Forthcoming*)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com
mroberts@bursor.com
vzhou@bursor.com

**BURSOR & FISHER, P.A.**
Joshua R. Wilner (State Bar No. 353949)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: jwilner@bursor.com

*Attorneys for Plaintiffs*